Exploring the suitability of IS security management standards for SMEs

Yves Barlette, GSCM-Montpellier Business School, France
y.barlette@supco-montpellier.fr
Vladislav V. Fomin, Vytautas Magnus University, Lithuania and RSM Erasmus University, The Netherlands
vvfomin@gmail.com

Abstract

In this paper we examine the adequacy of IS security standards to the needs of SMEs. Using the findings of literature review, we identify general criticism for the security standards. Further, we benchmark the recently published ISO 27001 IS security standard to ISO 9000 standard – a similar standard with a 20 years history – to develop expectations of how the future adoption of the recently introduced ISO 27001 standard can be fostered. We suggest, among other, that the legislative environment can play a crucial role for further growth of security standards adoption.

1. Introduction

The launch of policies for National Information Infrastructure (NII) development in the U.S., Europe, and Japan in the 1990s [37] is often considered as a departure point for Global Information Revolution [8] – creation of new global economies, where information play a doubly important role as both raw material and end product. Fuelled by the growth of Internet and the drastic diminishment of the PC unit price to its power ratio, the global informatization brought nearly ubiquitous adoption of PCs and Internet to large enterprises and SMEs alike [7].

The ratio and the role of computerized information in a contemporary company are often vital for company's daily operations and survival. Three quarters of the French companies reported a very strong reliance on their information technologies [12]. Information become more and more a synonym of patrimony, currency, and future of the company: historical data, research and development, standards, patents.

On the backdrop of the vital role the information and communication technologies (ICT) are playing in contemporary business, the average annual increase of ICT vulnerabilities reported by companies in leading post-industrial countries exceeds 45 percent per annum [10]. The high ratio of vulnerabilities highlights the fact that the ICT security issues are far from being solved. Management of a contemporary company is facing a problem of high dependence on the digitized information contrasted by the high risk of vulnerabilities.

The specifics of ICT-dependent business and the global competition drive firms to optimize and standardize their business processes [67], thus creating transparency and common reference points within and across firm boundaries [16]. Information Systems (IS) security methods and standards have emerged as a crucial component of good corporate governance [63]. However, due to the relative novelty of the issue, there is a call "for more empirical research to develop key principles for the prevention of negative events and to help in the management of security" [19].

In this paper, we address the issue of security methods or standards – tools "that enable to analyze, conceive, evaluate or control, together or separated, the security of information systems" [15]. One application of security methods includes guidelines and checklists allowing avoiding lapses and misses in the adoption/ implementation of security measures and procedures. Adoption of IS security methods or security standards' certification bears a direct interest of the company in developing *countermeasures* to IS-related vulnerabilities [3b]. An "indirect" aspects of adoption of IS security standards by a company is the creation of *awareness* of possible IS vulnerabilities and critical processes [3b].

Given the nature of contemporary business operation and global economy; one would expect to see growing certification of IS security standards in organizations. While relevant international standards exist, as for example International Standardization Organization's ISO 27001, the rate of IS security standards certification worldwide, and in France particularly, is surprisingly low.

In this paper we place the focus on the small and medium sized enterprises (SMEs) – companies employing not more than 250 employees. 97 percent of French companies fall into this category [31], while Europe-wide, SMEs represent 70 percent of the working force [59]. Our choice is justified not only by the sheer percentage of the SMEs in French business domain, but more so by the inadequately low adoption of IS security methods by SMEs. Less than 20 percent of French SMEs were reported to have defined an activity continuity plan or a crisis plan, which is much lower number than that for bigger companies [12]. SMEs are also reported to have

1530-1605/08 $25.00 © 2008 IEEE

more important discrepancies between the IS security measures implemented and actual security breaches: the emphasis is placed upon security measures against low probability risks instead of protecting themselves against the most frequent (and costly) problems [12].

Our research aim is to examine the adequacy of IS security standards in general, and ISO 27001 standard in particular, for SMEs. Our work is motivated by 1) companies' growing dependence on ICT in their daily business operations on the one hand, and high risk of ICT vulnerability on the other hand; 2) the low adoption rate of IS security standards by SMEs in France and worldwide; 3) the low awareness of companies' management of the benefits or disadvantages of having IS security measures implemented.

In order to deliver on the research goals, we conducted a literature review on existing IS security methods. We use the findings of the literature review to provide an analytic synthesis on the adequacy of existing IS security methods and standards for the requirements of SMEs. Finally, we draw on the past and present developments of similar to the IS security ISO 9000-series quality standards in the global economy to propose if and how the higher adoption of such methods and standards can be fostered.

2. IS security methods and standards

Over several decades there has been considerable research and development put into IS security methods, both in academia and by practitioners. As a result, many IS security policies, standards, and guidelines have been proposed, developed, and adopted by companies [9].

One application of (or motivation for adopting) security method is that it includes guidelines and checklists allowing avoiding lapses and misses in the adoption/ implementation of security measures and procedures, thus establishing countermeasures to IS-related vulnerabilities. A request from a partner firm (to keep a client-supplier partnership) or an insurance company (offering to lower an insurance indemnity) often becomes the leitmotif in creating incentives for adopting security methods or certifications.

In 1995 the British Standard Institution established BS 7799-1 standard titled "Information security part I: Code of practice for security management" and added in 1998 a second part, BS 7799-2 "Information security part II: specification for Information Security Management System (ISMS)". BS 7799-2 is a set of requirements for developing an ISMS that encompasses people, processes and IT systems. Both aforementioned BS standards were taken up by the ISO to become global ISMS standards. BS 7799-1 security standard was re-published in 2007 under the name of ISO 27002. BS 7799-2 became ISO 27001 standard in 2005. ISO 27001 can be viewed as an overall program that combines risk management, security management, governance and compliance. It helps an organization ensure that the right people, processes and technologies are in place that are appropriate to the business model and facilitate a proactive approach to managing security and risk [5]. The standard promotes strong values concerning the protection of client and business information.

ISO 27001 responds to business needs in establishing comprehensive ISMS policy, which allows not only harmonization of IS-related organizational processes, but also certification, thus establishing a common reference point for the certified company in the global market. However, adoption of ISMS standards is not a straightforward process for a company, least so for a SME. Recent research in this domain reveals important criticism for suitability and adaptability of security standards to business.

3. Research methods

This work combines the literature review method [64b] and system analysis method [2]. A review of prior relevant literature is an essential feature of academic project. It creates a foundation for advancing knowledge, facilitates theory development, and uncovers areas where research is needed [64b]. Given the scarcity of academic publications on the topic of suitability of IS security standards for SMEs, we found the literature review to be an adequate tool for exploring and synthesizing findings of prior research works.

The search for security standards and methods was conducted in the following way. First, the websites of French agencies such as DCSSI (French government I.S. security agency), CIGREF (Information systems big companies club), CLUSIF (French information systems security club) were examined for the references to French methods and their comparisons to other methods. The French agencies' websites also contained some rankings on the standards and methods. The rankings were later on used to develop Table 2 (see Appendix 1).

The second step involved examination of websites of European and the U.S. security associations and government agencies. Among these sites were such as CASES (Cyberworld awareness and security enhancement structure), ENISA (The European network and information security agency), CERT, BSI, SANS, and other. The third step involved examination of the websites of the standards and methods retrieved during the first

two steps of research: ISO, OCTAVE, ITIL, OSSTMM, CRAMM, COBIT, and other. This gave us access many professional articles, which otherwise wouldn't be listed in academic databases. Finally, the EBSCO and ABI/Inform databases were searched for scholarly publications using the combination of such keywords as "IS security", "standard", "method", "ISO 27001", and "ISO 9000". For articles which were found to be relevant, the reference lists were examined for locating further relevant works.

Through the literature review drivers and barriers to the adoption of IS security standards were identified. This allowed us to apply the system method [2] – to engage in discussing possible future development scenario for the success of ISO 27001 standard derived from identification of the driving forces of the system. However, we felt compelled to benchmark the identified drivers and barriers for the adoption of security standards to these of the similar past developments. Such benchmarking for the purpose of making analysis and predictions on the future state of a system is another application of a system method [2]. For the purposes of benchmarking, a well-known and widely adopted ISO 9000 quality standard was chosen.

We believe the comparison between the two different standards is justified, given that both standards are 1) process standards, which 2) are developed with common objectives, and 3) published by the same organization. A comparison of the two standards is provided in Table 1.

4. Literature review

In their study, [20] have rejected the hypothesis that the adoption of best ISMS practices (including ISO standards) by some organizations entails fewer security breaches in terms of both frequency and severity than those that have not. More generally they found almost no statistically significant relationship between the adoption of information security policies and the incidence or severity of security breaches [20].

Furthermore, for successful adoption of ISMS standard, security policies must be tailored to the culture of the organization [29, 33], well aligned with corporate objectives [33, 48] and rigorously enforced [17, 20]. In other words, while ISMS policies are published as uniform standards (or norms), in the real business environment requirements for these standards will differ [4], depending on the specific organizational context and type of information being processed [47, 51, 65].

[38] highlight the need to measure information security at the management and business level. The information security culture and the climate are very important concepts [46, 60], which would affect the implementation of ISMS. Thus, [38] recommend addressing this issue before implementing directly the in-depth procedural controls included in standards. [19] consider that security standard's "checklists emphasize observable events and focus attention to procedure without considering the social nature of the problems and without addressing the key task of understanding what the significant questions are."

Without consulting managerial processes first, adoption of security standard can result in utopian security culture where the employees of the organization are expected to follow the guidelines of the organization voluntarily as part of their second nature [64]. In such situation, the ISMS policies may not impact users on the ground, which will result in a standard adoption failure [29]. In other words, "one way to ensure that employee actions, behaviour, artifacts and creations are according to company policies is to align these with company culture" [62].

Standard and organizational culture alignment require several important managerial interventions. First, an awareness of the expected/desired outcomes of ISMS policy adoption must be created. [52] and [66] emphasized the fact that if employees are not made aware of a policy, there is a danger that it will become a dead document rather than an active and effective security management tool. Second, employees need to be educated and trained (the what, why, and how) on the security aspects required in information security policy [38]. Employees must know how to behave correctly, how to use the security tools, security functionalities included in software, and the security implicated in their own day-to-day processes [50].

4.1. Suitability of security methods and standards for SMEs

By the end of August 2007, there were only five ISO 27001 certified companies in France, which is considerably below these numbers for U.K., Germany, and the U.S. (352, 73, 52 respectively), and which places France at about the 30th rank worldwide [32].

At the backdrop of the general criticism received for IS security methods, and the negligent rate of security standards certification in France, we next explore the suitability of ISMS standards to the specific characteristics of SMEs, which comprise 97 percent of French companies [31], and represent 70 percent of the working force Europe-wide [59].

The problem of ISMS implementation in SMEs is a versatile one. In their survey, [24] highlight three crucial elements pertaining to IS security that characterize SMEs:

- an increasing interdependency between firms (partners, clients, vendors, third party), and the necessity for each company to be reassured on other companies information security;
- companies are driven by a more and more competitive environment to adopt emerging and immature technologies, carrying threats;
- a widening gap between increasing risks and the deficiency of countermeasures to cope with them.

The findings of the survey [24], especially with respect to few countermeasures implemented by SMEs compared to bigger companies, should not be surprising. SMEs face problems in recruiting qualified employees [41, 44], are challenged more than large companies in evaluating possible IS-related risks [28], and lack information security awareness [40].

SMEs have dynamic business environments [51, 55] and, according to [54], existing studies on IS security policies pay little attention to how to deal with exceptional situations in which IS security policies are in conflict with the business objectives of organizations. The unpredictability of the business environment drives SMEs to make rapid business decisions with little preparation [36].

[53] argues that standards have an important limitation, because "they focus on ensuring that certain information security processes or activities exist, while they are unconcerned about and fail to give advice on how these security processes can be accomplished in practice." Furthermore, a standard is too general to offer an explicit advice on how the policy might best be aligned with specific corporate objectives [21].

SMEs generally lack computer experience and do not have sufficient internal IS expertise [18, 27, 56]. This situation is precipitated on difficulties in recruiting and retaining internal IS experts due to scarcity of qualified IS experts and limited career advancement prospects offered by SMEs [58]. As a result, SMEs are driven to outsource the necessary competences [55], which they cannot afford [61].

Effective security management requires a great deal of time, effort and money, which most of SMEs are not prepared to commit [20, 42]. Security standard's implementation can take more than 5 or 6 months [13], not least so due to a very complex nature of security standards [1].

To summarize, we find the following quote from ENISA[1] to be a quite comprehensive statement on the problem of IS security standard suitability for SMEs:

"A simple approach designed for small organizations does not exist today, at least not in the form of publicly available guidelines. Some consulting firms have developed good practices for that purpose, but they use them within customer projects. Other approaches, although claiming to be appropriate for SMEs, are still too complex for self-assessments… On the other hand most SMEs cannot afford the cost of fully outsourcing this function to external parties." [23]

5. Analysis

In this section we attempt to reveal the factors for low adoption of IS security standards in general, and ISO 27001 in particular. The general criticism found in literature reviewed suggests that companies in general, and SMEs in particular, are not well positioned to adopt ISMS standards. However, in the tradition of system sciences, we believe important insights on the drivers and barriers to standards adoption can be obtained from similar past developments. A systemic approach to complex organizational problems is to develop expectations of how the future will unfold and to define actions that would lead to more desirable predicted futures [2]. This approach requires an expert knowledge from similar past developments. In this respect, we find that benchmarking the ISO 27001 standard to its well known predecessor, ISO 9000-series quality management standard, can inform us on future adoption of the former.

Development of both ISO standards was motivated by the need of giving a unique and coherent international configuration to business processes, namely to the quality assurance (ISO 9000) and to the IS-related security (ISO 27001). The aim for developing (and adopting) these standards is to facilitate the growth of global markets by harmonizing terms, systems and methodologies. ISO 9000 standard has been published in 1987, and after two decades of seeing a growth of adoption, is probably reaching the end of its lifecycle, as depicted by down slope of the cumulative adoption curve [34, 35]. The ISO 27001, on the other hand, is in its early stage of adoption, being first published in 1998 as a British national standard, and only in 2005 as an international ISO standard.

In only few years after its first publication, ISO 9000 became the leading reference for quality system organization all over the world. Given the familiarity of global businesses with the ISO standards due to the success of its 9000 series, and the importance of ISMS

[1] European Network and Information Security Agency

issues in contemporary business, it is surprising to find that the ISO 27001 has not seen as wide recognition as its predecessor. Also, ISO 27001 seems to fare worse than some of its contemporary counterparts, such as e.g., environmental management ISO 14001 standard.

5.1. Common critical factors for the ISO 9000 and 27001 standards adoption

By the end of 2005, more than 775.000 certificates for ISO 9000 had been issued in 161 countries, with an annual growing rate close to 10-15 percent [35]. However, we may infer that the certification market for ISO 9000 is coming to saturation, and even to end of life cycle in most of the developed countries. Also, the saturation level represents only a fraction of the total number of corporation companies. The empirical saturation values for U.K., Germany and France, respectively, were 9, 8 and 2 percent of corporation companies during the upslope of the cumulative adoption curve [26]. Today, the number of certificates is lowering, resulting in the down slope of the cumulative curve [34, 35]. The driving push begins to attenuate under the effect of some factors: the reduction of the competitive gap between certified and not certified companies, and the limited number of enterprises potentially interested to certification [26].

Critical success factors for companies seeking to obtain ISO 9000 certification were identified as the following [3]:

- proper driving force towards obtaining the ISO 9000 certification;
- expert advice and uniqueness of the system, reflecting the nature of the company's operation [39];
- internal and external customer focus;
- value-added approach to quality cost;
- use of the standard in an integrated manner [57];
- positive attitude towards ISO 9000 on the part of staff;
- dynamic approach to quality improvement;
- presenting ISO 9000 in an easy manner to the employees [14].

The aforementioned critical factors are coherent, if not identical, to those identified in the literature review on ISMS standards, as reported above. Another commonality is the special position of SMEs in adoption of the standard - SMEs face particular difficulties with gaining ISO 9000 series certification, where the lack of commitment of employees, managers and time commitment is the most frequently mentioned problem [6].

Further commonalities are found in the complexity of the standards - ISO 9000 series standards cannot be easily understood by a non-professional person, and there are difficulties in understanding exactly what the standard requires and inconsistencies with the interpretation of standards by consultants and assessors [6].

The cost of the standard presents another common point of reference - ISO 9000 series qualification is generally an expensive process for SMEs as they are more reliant on outside assistance [6].

The issue of generality of guidelines vs. specificity of business processes is also not a unique problem of security standards - ISO 9000 standards only give a set of general/generic guidelines, but they do not guarantee that the process is durable, capable and mature in the application of related constructs [26].

5.2. Differences between the ISO 9000 and 27001 standards

An Important difference is the target business sector. ISO 9000 series were aimed at manufacturing-related process standardization, while ISO 27001 is more generic, IS-process oriented.

The top three sectors in 2002 for ISO 9000 adoption were construction, basic metal and fabricated metal (due to the large influence of automotive industry), and electrical and optical equipment [26]. It is tempting to assume that the high rate of adoption by these sectors is prompted by the liability-prone nature of the business, and "regulatory/legislation effect". Many countries impose ISO 9000 certification for participating to public-work contracts. Until recently, construction has not been IS-intensive business sector, and hence we cannot expect it to assume the leading rank in ISO 27001 adoption.

5.3. Drivers for adoption

Quality certification contributes to business performance when the quality culture in the organization is well developed and the manager's motivation to gain the certification is to improve business performance and not to conform to a standard. [26].

We can find the same aspect in ISMS certification in the improvement of the security of the information assets. The stock market reacts positively to a quality certification. Quality certification can be considered as a useful tool for reducing the information asymmetry between buyers and sellers, as well as a strategic element for the companies to distinguish themselves in the business competition [43], by giving an external and formal evidence of their organizational efforts towards quality practice [26].

However, if security certification is considered as leverage for confidence between companies [11, 45] engaged in business transactions, the literature review does not reveal the presence of the distinguishing effect for adopting companies in the business competition nor any positive reaction of the stock market.

A correlation among quality certification and business performances is not univocally demonstrable. Is the increase of business due to the management methodology prescribed by quality standards or is certification a way for distinguishing itself in a global market [26]? More so, the low threshold level for certification saturation suggests that when the number of certified organizations reaches a certain limit, certification loses its connotation and becomes less attractive for the remaining companies [26].

The security certification has been designed for the protection of IS. Therefore, similarly to the quality standards, quantification of benefits of ISMS standard adoption is problematic. The interest of a security standard is to prevent the security failures and to mitigate their consequences.

The most significant benefits of a quality certification are in terms of raising quality awareness in an organization. This reinforces the view that certification is a good foundation upon which to start the quality improvement process. Surveyed ISO-certified SMEs rank improved awareness of problems and improved customer service come as 2nd and 3rd respectively. On the contrary, such factors as improved market share, reduced costs, and help in international market rank 18, 21, and 23, respectively [6].

The benefits of a security certification are very similar on this point: they raise the security awareness and facilitate a gradual improvement of the security [45].

In the near future, the benefits of ISO 9000 certification will only depend on the good use of the quality management system that has been implemented to obtain the certification rather on the mere certification as a signal to markets [49]. This is already the case for ISO 27001 and the good use of the ISMS.

5.4. Barriers to adoption

SMEs managers over-evaluate and exaggerate the possibilities of quality certification and their expectations are thus unrealistic. This give rise to their dissatisfaction when the results do not measure up their plans.

This dissatisfaction might be even higher for SMEs given that they find more barriers to achieve and exploit certification [49]. As security standards adoption and certification are almost seen as expenses, dissatisfaction for these motives is not imaginable.

The greatest disappointment for an enterprise is to discover that, having achieved quality certification, a non-certified company has been awarded a contract by a customer or government body who required suppliers to be certified [6]. It is likely to lead to disillusionment with ISO 9000 particularly given the high cost of certification both in terms of money for consultants and audits and extra employees or overtime required in relation to the certification [6].

We didn't find any evidence for such kind of disappointment though the high costs in money and time of ISMS standards implementation have also been outlined. In quality certification, disappointment comes from the increase in paperwork [6], which is different in the security certification process, which is less of a "paper-generator."

The higher expectations of small companies with respect to ISO 9000 certifications refer to commercial aspects: access to new markets, increase of market share and business portfolio, image improvement, and so on. However many of these objectives depend on the differentiating power of certification. Such power was significant when ISO 9000 certification was not widely extended and the certified companies stood out from the others. This differentiating power has fallen and empirical data have shown that this effect results in lower commercial advantages and higher dissatisfaction of small businesses managers with respect to ISO 9000 certification [49].

Any competitive advantage to a single enterprise may be short lived, as it is usually only a matter of time before many companies in the same industry achieve certification. It is then seen by many as just another cost of doing business without any corresponding improvements in market share [6].

If however, the manager of the business sees certification as an opportunity to improve internal processes and systems from the outset rather than a mechanism to get a certificate on the wall, it is likely to yield positive results [6].

Furthermore, in this situation, employees are more likely to be involved in developing the system with the assistance from external consultants. It becomes a workable system which has the commitment of employees [6].

6. Conclusions

In this paper we examined the adequacy of IS security standards to the needs of SMEs and attempted to reveal critical drivers and barriers for standard certification. Through the literature review, we have identified general criticism for the security standards. Further, in the tradition of a systemic approach to complex organizational problems [2], we compared the pros and cons of a recently published ISO 27001 IS security standard to those of similar standard with a 20 years history. Through this benchmarking, we can develop expectations of how the future adoption of the recently introduced ISO 27001 standard will unfold, and propose actions that would lead to more desirable predicted futures [2].

Overall, we find that the general negative issues pertaining to IS security standards, as revealed in the literature review, should not become inhibitors to the standards adoption. It appears that ISO 9000 standard has seen a steady increase of adoption over the years despite receiving virtually the same criticism as that we find for ISO 27001 standard.

We argue that it is the legislative environment and the ability to quantify the benefits from adopting the security standards, which can be a driver for further ISO 27001 adoption. The specifics of business processes and risk-taking nature of entrepreneurial activity should also be paid attention to when developing incentives for the standards adoption.

As an example of legislative environment factors, the dissemination of ISO 9000 was promoted by central governments and by national bodies, reducing administrative features and supporting the diffusion of the certification bodies in the countries [26] – the same can / should be done for ISO 27001.

Liability-prone sectors are the leading sectors of ISO 9000 adoption – national IS-related legislation can drive the ISO 27001 (and similar standards) adoption.

ISO 9000 represents a universal quality tool for a global market. On the contrary, security methods are numerous and ISO 27001 corresponds to only one method, with its qualities and drawbacks as it can be seen in Table 2 (Appendix 1).

As an example of quantification issue, we can assume that it is very difficult to prove the security standards' usefulness. Contrary to quality certification that has been and remained an important distinguishing factor due to a possibility to establish a quantifiable link between the quality increase and business increase, the reduction of the security failures entailed by an increase in information security is virtually impossible to quantify. Information security differs from quality in another peculiar way – the level of quality can be measured in positive terms, whereas the level of security is better measured as the "level of insecurity", that could be assimilated to the risk level, made from the probability of occurrence of threats and vulnerabilities [47b].

Finally, we believe that the specifics of the business process, namely the degree of presence of liability risk, presents an important distinguishing factor between the quality and security standards. While the top-three sectors leading the ISO 9000 certification are all heavily affected by liability in case of product failure or malfunction due to poor quality (construction, automotive), the liability for poor IS security management is not well established as a practice.

There are normative acts like Sarbanes Oxley Act, but they only apply to companies in relation with security exchange commission, and most SMEs are not supposed to have these relations. French laws (which are complying with European laws) such as CNIL, and articles 226-16 to 226-22 of the French "code penal" can penalize with 3 to 5 years in prison and € 100.000 to € 300.000 fines the companies having an insufficient data protection, but most SMEs managers are unaware of these laws and their implications! And such a penalty can only be imposed when a security breach have disserved clients or employees with severe consequences. We suggest that European and French policy-makers should develop constructive methods for dissemination of knowledge on IS security legislation to businesses, and SMEs in particular. Constructive approach is needed to counter-balance the risk-taking psychological profile of SMEs' managers [36].

Table 2 shows that few standards are theoretically suitable for SMEs, and their actual fit is denied by [23]. Given the cost, the skills needed and the language issues, we can assume that there is no method today that can help the SMEs to improve their security. This fact is aggravated when we take into account that 97 percent of French companies are SMEs.

However, in this paper we have demonstrated that there is a number of important drivers for IS security standards adoption, some of which are already in place, and some can be installed by appropriate action. Given the situation, we call for more research directed at creation and adoption of simplified security methods or standards at academic and managerial level in order to create a framework of certification dedicated to SMEs.

Specifically, they suggest that there is a need for having at least 2 versions of the standards: one suitable for big SMEs and big companies, one for small SMEs. simplified in terms of time, money and certification cost.

Further, standard adoption guide should be created by standard's developers, presenting the "real benefits" and the "false expectations" (e.g., "don't over-evaluate the competitive impacts of certification. Simply assuring good practices may be is more relevant for your business).

Finally, social aspect of standard's adoption must be emphasized. For example, the impact that managers' commitment to the standard's adoption process can have, the impact of creating awareness of security failures and benefits of having security standard in place, etc. In other words, education and training of employees should be fostered.

7. References

[1] Arnott S., (2002), Strategy paper, Computing, (Feb).

[2] Axelrod, R. M. and Cohen, M. D. (1999), Harnessing complexity: organizational implications of a scientific frontier, Free Press, New York

[3] Augustyn M. M., and Pheby J.D., (2000), "ISO 9000 and performance of small tourism enterprises: a focus on Westons Cider Company", Managing service quality, Vol. 10 (6), 2000, pp. 374-388.

[3b] Barlette Y., (2006), Les comportements sécuritaires des acteurs dans les systèmes d'information des PME. Thèse de doctorat en sciences de gestion, université de Montpellier I.

[4] Baskerville, R. (1993), "Information systems security design methods: implications for information systems development", ACM Computing Surveys, Vol. 25 No.4, pp.375-414.

[5] Brenner J., (2007), "ISO 27001: Risk management and compliance", Risk Management Magazine, Vol. 54 (1), pp. 24-29;

[6] Brown A., Van der Wiele T., Loughton K., (1998), "Smaller enterprises' experiences with ISO 9000", International journal of Quality & reliability management, Vol. 15 (3), 1998, pp. 273-285.

[7] Brousseau, E., (2002), "Globalization and E-commerce: The French Environment and Policy", Center for Research on Information Technology and Organizations (CRITO), University of California, Irvine. http://www.crito.uci.edu/publications/pdf/GEC2_France.pdf

[8] Castells, M. (1996), The Rise of the Network Society, Blackwell Publishers, Ltd, Oxford

[9] Chapman D., Smalov L., (2004), "On information security guidelines for small/medium enterprises", ICEIS 2004 – Information analysis and specification, 2004, pp. 3-9.

[10] CERT, (2007), "*CERT/CC: Statistics 1988-2007",* Computer Emergency Response Team, www.cert.org, USA;

[11] CIGREF, (2002), Sécurité des systèmes d'information: quelle politique globale de gestion des risques?, September, www.cigref.fr, Paris

[12] CLUSIF, (2004; 2006), *"Politiques de sécurité des systèmes d'information et sinistralité en France"*, Club de la sécurité des informations français (French information systems security club), Paris.

[13] CNRS, (2002), "La certification des critères communs: le point de vue du developpeur", Securité informatique, N° 42, pp. 5-6.

[14] Conway T., (1994), "BS 5750 – a logical step", The TQM magazine, Vol. 6 (5), pp. 38-40.

[15] DCSSI, (2007), Direction centrale de la sécurité des systèmes d'information (Information systems security central agency), http://www.ssi.gouv.fr/fr/dcssi/;

[16] Davenport, T. H., (2005), "The coming commoditization of processes," Harvard Business Review (June), pp. 100-108.

[17] David J., (2002), "Policy enforcement in the workplace", *Computers & Security,* Vol. 21 (6), pp. 506-513;

[18] DeLone W.H., (1988), "Determinants of success for computer usage in small businesses", *MIS Quarterly*, Vol. 5 (4), pp. 51-61;

[19] Dhillon G., Backhouse J., (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, 11, pp. 127-153;

[20] Doherty N.F., Fulford H., (2005), "Do information security policies reduce the incidence of security breaches: an exploratory analysis", *Information resources management journal*; 18 (4), Oct-Dec, pp. 21-39;

[21] Doherty N.F., Fulford H., (2006), "Aligning the information security policy with the strategic information systems plan", *Computers & Security*; 25, pp. 55-63;

[22] ENISA, (2006), "Risk management implementation principles and inventories for risk management / risk assessment methods and tools", June;

[23] ENISA, (2007), "ENISA deliverable: Information Package for SMEs", February;

[24] Ernst & Young, (2005), "La gestion des risques dans l'actualité du contrôle interne : pratiques et tendances", mai 2005;

[25] Franceschini F., Galetto M., Gianni G., (2004), "A new forecasting model for the diffusion of ISO 9000 standards certifications in European countries", International journal of Quality & reliability management, Vol. 21 (1), pp. 32-50.

[26] Franceschini F., Galetto M., Cecconi P., (2006), "A worldwide analysis of ISO 9000 standard diffusion: Considerations and future development", Benchmarking: An international journal, Vol. 13 (4), pp. 523-541.

[27] Gable G.G., (1991), "consultant engagement for first time computerization: A proactive client role in small businesses", *Information & Management*, Vol. 20, pp. 83-93;

[28] Gupta A., Hammond R., (2005), "Information systems security issues and decisions for small businesses: an empirical examination", *Information Management and Computer Security*, Vol. 13 N°4, pp. 297-310;

[29] Hone K., Eloff J.H.P., (2002a), "What makes an effective information security policy", *Network Security*, Vol. 20 (6), pp. 14-16;

[30] Hone K., Eloff J.H.P., (2002b), "Information security policy: what do international security standards say", *Computers & Security*, Vol. 21 (5), pp. 402-409;

[31] INSEE, (2007), Caractéristiques des entreprises industrielles de 20 salariés ou plus, www.insee.fr (French national institute of statistics and economic surveys);
[32] ISMS User Group, (2007), http://www.iso27001certificates.com/.
[33] ISO, (2000), Information Technology. Code of practice for information security management, ISO 17799. International standards organization;
[34] ISO, (2002), "The ISO survey of ISO 9001:2000 and ISO 14001 Certificates", Twelfth cycle, Geneva.
[35] ISO (2003, 2004, 2005), "The ISO survey of ISO 9001:2000 and ISO 14001 Certificates", Geneva.
[36] Julien P.A., Marchesnay M., (1988), *La petite entreprise*, Vuibert, Paris;
[37] Kahin, B. (1997), "The U.S. National Information Infrastructure Initiative: The Market, the Net, and the Virtual Project", in Kahin, B. and Wilson, E. (Eds), Nati*onal Information Infrastructure Initiatives: Vision and Policy Design, MI*T Press, Cambridge, Mass.
[38] Martins, A., Eloff, J.H.P., (2001), "Measuring Information Security", *Proceedings of Workshop on Information Security – System Rating and Ranking*, Virginia;
[39] Mc Lachlan V.N., (1996), "In praise of ISO 9000", The TQM magazine, Vol. 8 (3), pp. 21-23.
[40] Mitchell R.C., Marcella R., Baxter G., (1999), "Corporate information security management", *New Library World,* Vol. 100, n°1150, pp. 213-227, MCB University press;
[41] Monnoyer M.C., (2003), *Le dirigeant confronté à la décision d'investissement en T.I.C.*, in Boutary, TIC et PME : des usages aux stratégies, l'Harmattan, Paris;
[42] Moule B., Giavara L., (1995), "Policies, procedures and standards: an approach for implementation", *Information Management & Computer Security*, Vol. 3 (3), pp. 7-16;
[43] Nicolau J.L., Sellers R., (2002), "The stock market's reaction to quality certification: empirical evidence from Spain", European journal of operations research, Vol. 142, pp. 632-41;
[44] Noteboom B., (1988), "The facts about small business and the real values of its 'life world'", *American journal of economics and sociology* (47:3), July 1988, pp. 299-314;
[45] OECD, (2002), "OECD Guidelines for the Security of Information Systems and Networks", 30p;
[46] Nosworthy J.D., (2000), "Implementing information security in the 21st century – Do you have the balancing factors?", *Computers and security*, Vol. 19 (4), pp. 337-347;
[47] Pernul G., (1995), "Information Systems Security: Scope, State-of-the-art, and Evaluation of Techniques", *International journal of information management*, Vol. 15 (3), pp. 165-180; [47b]
[47b]Pipkin D., (2000), Sécurite des informations, Campus Press, Paris.
[48] Rees J., Bandyopadhyay S., Spafford E.H., (2003), "PFIRES: A policy framework for information security", *Communications of the ACM*, Vol. 46 (7), pp. 101-106;
[49] Rodriguez-Escobar J.A., Gonzalez-Benito J., Martinez-Lorente A.R., (2006), "An analysis of the degree of small companies' dissatisfaction with ISO 9000 certification", Total quality management, Vol. 17 (4), pp. 507-521.
[50] Schlienger T., Teufel S., (2003), "Information security culture: from analysis to change", South African Computer Journal, Vol. 31, pp. 46-52;
[51] Schweitzer, J.A. (1982), Managing Information Security: A Program for the Electronic Information Age, Butterworth-Heinemann, Boston, MA.
[52] Siponen M.T., (2000), "Policies for construction of information systems' security guidelines" in *proceedings of the 15ht information security conference (IFIP TC11/Sec 2000)*, Beijing, China, August, pp. 111-120;
[53] Siponen M.T., (2006), "Information security standards focus on the existence of process, not its content", *Communications of the ACM*, Vol. 49 (8), pp. 97-100;
[54] Siponen M.T., Iivari J., (2006), "Six design theories for IS security Policies and Guidelines", *Journal of the Association for Information systems*, Vol. 7 (7), pp. 445-472;
[55] Soh C.P.P., Yap C.S., Raman K.S., (1992), "Impact of consultants on computerization success in small businesses", *Information and Management*, Vol. 22, pp. 309-319;
[56] Spinellis D., Kokolakis S., Gritzalis S., (1999), "Security requirements, risks and recommendations for small enterprise and home-office environments", *Information Management and Computer Security,* Vol.7 N°3, pp. 121-128*;*
[57] Subba R., Ragu-Nathan T.S., Solis L.E., (1997), "Does ISO 9000 have an effect on quality management practices? An international empirical study", Total quality management, Vol. 8 (6), pp. 335-346.
[58] Thong J.Y.L, Yap C.S., Raman K.S., (1996), "Top management support, external expertise and information systems implementation in small businesses", *Information systems research*, Vol.7, N° 2, pp 248-267;
[59] Turner C., (1997), "SMEs and the evolution of the European information society: policy themes and initiatives", *European Business Journal*, Vol. 9, N° 4, London; pp. 47-52;
[60] Von Solms B., (2000), "information security- The third wave?", *Computers & Security*, Vol. 19 (7), pp. 615-620;
[61] Von Solms R., Van de Haar, (2000), "*From Trusted Information Security Controls to a Trusted Information Security Environment"*, proceeding of the 16th Annual Working Conference on Information Security, IFIP, August, Beijing, Chine, contribution n°4/52;
[62] Von Solms B., Von Solms R., (2004), "From policies to culture", *Computers & Security*, Vol. 23, pp. 275-279;
[63] Von Solms B., Von Solms R., (2005), "From information security to … business security", *Computers & Security*, Vol. 24, pp. 271-273;
[64] Vroom C., Von Solms R., (2004), "Towards information security behavioural compliance", *Computers & Security*, Vol.23, pp. 191-198;
[64b] Webster, J., & Watson, R. T. (2002). "Analyzing the Past to Prepare for the Future: Writing a Literature Review", *MIS Quarterly, 26*(2), xiii-xxiii.
[65] Wood, C.C. (1999), *Information Security Policies Made Easy*, Baseline Software, San Rafael, CA.
[66] Wood CC., (2000), "An unappreciated reason why information security policies fail", *Computer fraud & Security*, Vol. 2000 (10), pp. 13-14;
[67] Wüllenweber K., and Weitzel T., (2007), "An empirical exploration of how process standardization reduces outsourcing risks", *Proceedings of the 40th annual Hawaii International conference on system sciences (HICSS'07)*

Appendix 1

Table 1: Comparison of ISO 27001 and ISO 9000 standards

	ISO 27001	**ISO 9000**
Domain of application	IS- related process security	Manufacturing and service process quality
Topic necessary to improve	Information assets security	Business performance
Main target of the standard	IS dependant companies	Mainly manufacturing (*) related companies
Creation date	2005 (1998 as BS 7799-2)	1987
Position in lifecycle (most developed countries)	Beginning of lifecycle	End of lifecycle
The role of liability as a driver for adoption	Unimportant	Important
Failure detection	Security failures can exist without being detected	Failure is easy to detect
Legal or business related consequences of the failure	Awareness of managers on the possible consequences of failure is very low	Awareness of managers on the consequences of failure is adequate
Motivations for adoption / success factors in small SMEs		
Request of another firm	x	x
Request/incentives of government bodies	Very little number of SMEs (in France) has been mandated to adopt security standards	Governments played a visible role in creating incentives for standards' adoption by companies
Competitive gap between certified and not certified companies	Certification can become a burden due to the lack of resources for standards' adoption	Low today in developed countries
Requires employees' and managers' commitment	x	x
Possibility to measure the impact on application domain's performance	Level of security is very difficult to measure, no adequate measures exist	Level of security is easy to measure, adequate measures exist
Barriers to adoption in small SMEs		
Lack of skilled resources	x	x
Time Needed	x	x
Complexity of the standard	x	x
Cost of the process of certification	x	x
Quantification of benefits	Difficult	Difficult
Over-evaluation of benefits leading to dissatisfaction	No or very low	Yes
Increase in paperwork	Not important	Noticeable
Number of methods	Many national and international methods (**)	Universality of ISO 9000

(*) Top three sectors : construction, basic and fabricated metal (automotive), electrical equipments [26]
(**) See table comparing security methods and standards

Table 2: Methods and standards.

Name	Company size (*)	Creation date	Necessity	Cost (Money)	Skills needed	Language issue
BS 7799 1 & 2	C, B	1995	N.M.	N/A	**	E
COBIT	C, B	1996	N.M.	ISACA Members	**	I
CRAMM	C, B	1990	For G.O.	2200 Ū + 365 Ū (#)	***	E
EBIOS	C, B	1995	For G.O.	Free	**	I
ISF Methods	C, B	1996	N.M.	ISF Members	* to ***	E
ITIL / BS 15000	C, B	1989	N.M.	Free	N/A	I
ITBPM	C, B	1994	N.M. Certification possible	Free	**	E, German
MEHARI	C, B	1996	N.M.	100-500 Ū	**	E, French
NIST SP 800-30	C, B	2002	N.M.	Free	**	E
OCTAVE	C, B. S (?)	1999	N.M.	Free	**	E
OSSTMM	C, B. S (?)	2001	N.M.	Free	* to **	E, Spanish
PSSI (PSI: 1994)	C, B	2004	For G.O.	Free	**	French
SSE-CMM (ISO 21827)	C, B	1996		130 Ū	** to ***	E
ISO standards						
ISO 13335-2 (ISO 27005)	C, B	1996	Standard only	100 Ū	**	E
ISO 15408	C, B	1996	ISO Certification possible	90-285 Ū (3 parts)	N/A	E
ISO 27001 (BS 7799-2)	C, B	2005	ISO Certification possible	80 Ū	**	I
ISO 27002 (ISO 17799 - BS7799-1)	C, B	2005	Standard only	130 Ū	**	E

(*) C: Civil service, B: Big company, S: Small business
GO: Government organizations
NM: Not Mandatory
#: annual licence
* : basic level
** : standard level
*** : specialist level
I: International
E: English

Adapted and updated from [22].