

Positive and Negative Findings of the ISO/IEC 17799 Framework

Timo Wiander
Department of Information Processing Science
University of Oulu
Oulu, Finland
Email: timo.wiander@oulu.fi

Abstract

The ISO/IEC 17799 standard is commonly viewed as a necessary element in information security management. However, there is no empirical evidence of the usefulness of the standard in practice. To study this issue, this study analyses the implementation experiences of four organisations that have implemented the ISO/IEC 17799 standard. Through semi-structured interviews, the results of the study suggest that clients' needs and competitive advantage are the major reasons for implementing the standard. Furthermore, the implementation of the standard has increased the understanding of information security in all personnel groups and the understanding of security has broadened from the technical aspects to corporate security. As downsides of implementing the ISO/IEC 17799 standard, the costs and increased amount of work were mentioned as the worst. In addition, the difficulties in deploying the standard, and the readability of the standard were criticised. The standard was also criticised because it does not directly affect the quality of the end product or service; it only has an indirect effect owing to the improved information security practices.

Keywords

ISO/IEC 17799 standard, information security management

Introduction

Information security management is a challenging task and requires multidisciplinary expertise to succeed. While implementing technical countermeasures, such as firewalls and virus protection, one must take a broad look at an organisation, its assets, processes and resources. Protection of all those dimensions is crucial from the business continuity point of view. Globalisation, global competition and global exposure to threats mean that organizations have to cover a vast variety of threats, including hacking, denial of service attacks, frauds, viruses and other malware, espionage, insider threats, social engineering and so on (Deloitte 2005; Ernst & Young 2005; Im & Baskerville 2005; Whitman 2003; Shephard 2002; Theoharidou *et al.* 2005; Bishop 2005; Barber 2001).

Huge amounts of information are exchanged between and within organisations. The information itself is getting more value as an asset and this is a key reason why information security is increasingly becoming an important issue (ISO/IEC 17799 2005; Gerber & von Solms 2005; Siponen 2005). Furthermore, external parties demand management actions to be taken for securing information security, for example Sarbanes Oxley Act (SOX) and Basel II are examples of such demands from regulators (Pinder 2006; O'Connor 2005; Schultz 2004; Sutton & Arnold 2005; OECD 2006; Homeland 2006; Relyea 2004). The agreements between organisations also set their demands on management: it must be clearly understood how information security issues in the complex and dynamic world of sub-contractors and clients are handled, and how third parties can be assured that information security is in solid hands within the organisations' own perimeter.

All these premises lead to the protection of the core issue, the information itself. Technical protection without systematic planning and management is not enough. To use standards is one way to aid practitioners in such systematic planning. In fact, standards in general are argued to be the enabler of innovation and facilitator of technological change, and they have positive economic impact - for example, 13% of the growth in labour productivity is attributed to the role of standards (DTI 2005). There are several frameworks or best practices to choose from in the area of information security management. The ISO/IEC 17799 (2005) standard is commonly used (see e.g. Ernst & Young 2005; Xisec 2006) and its significance has been pointed out among practitioners (Tong *et al.* 2003) and cited by the academy (see e.g. Siponen 2006; von Solms 2005; von Solms 2001; von Solms 1999). And yet despite all this, there is no empirical research exploring the real usefulness of the standard in practice.

This study aims to fill this gap in the research by exploring how the practitioners perceive the ISO/IEC 17799 (2005) standard as an information security management framework. The qualitative research method was chosen as the research method for finding answers to the research question. Since the standard is seen as the silver

bullet of IS security management, this study contributes to the practice by critically unveiling tried and tested principles for applying IS security management standards in organisations.

Semi-structured interviews (Hirsjärvi & Hurme 2000; Eskola & Vastamäki 2001) were used for conducting the empirical part of this work. The semi-structured interview research approach was chosen since it can capture the process nature of the phenomena and also allows revising the research plan during the entire research time (Eskola & Suoranta 2001, 15-16). The strength of the semi-structured interviews is in the richness of information, which can be obtained in real-life situations (Eskola & Suoranta 2001). This was seen as an advantage because there is no prior research on practitioners' experiences of the use of the ISO/IEC 17799 (2005) standard in practice.

Positive Reasons for Why ISO/IEC 17799 was selected as the Framework

The most important reason for acquiring an ISO/IEC 17799 (2005) certificate was to respond to the pressure from third parties, namely from the clients. Other important reasons were to get competitive advantage, support for sales efforts and to get a security framework. The positive reasons are listed in Table 1.

Table 1: Positive reasons for selecting ISO/IEC 17799 (2005)

Positive reason	Mentions
Client demands.	5
Competitive advantage.	4
Support for sales efforts.	4
(Formalised) Security framework.	4
Implementation of best practice.	2
System can be certified.	2
Good public name.	2
Risk-based approach to information security.	2
Risk management.	2
Overall quality.	2
External quality support and presentation.	1
Compliance with internal policy.	1
Meeting governmental requirements.	1
Internationally known framework.	1
Rise of overall security level.	1
Driving force for security issues.	1
Shows the management's internal commitment to security.	1

All interviewees raised *the client* as the driving force, and they wanted to fulfil the client's expectations. One interviewee mentioned that there was pressure to get the certificate:

R: "... we wanted to be a subcontractor in (business sector) for big companies abroad ...it was an ultimate requirement." (R1)

Even though the interviewees perceived pressure from the clients, they did not mention that this pressure was negative. On the contrary, one interviewee commented that they wanted to foresee the client demands. *Competitive advantage and support for the sales efforts* of the company were raised as major drivers within these organisations, so the ISO/IEC 17799 (2005) standard was also seen as a marketing or sales tool. *Formalised security framework* was also mentioned as an important reason for implementation of the standard. The security framework even changed the work practices:

R: "...we started to have real meetings with minutes ...before, e-mail was whirling around and then we maybe had agreed something (laughs)." (R3)

Not only had the work practices changed, the standard also aided decision making and tracking by formalising the meetings and guaranteeing that they were held promptly and minuted. The interviewee emphasised that the ISO framework itself was an asset to the organisation. It gave them the means to evaluate the current situation in a systematic way. One of the interviewees mentioned that the framework could be utilised as an analysis tool:

R: "...glasses to look at information security." (R1)

According to the interviewee, the standard gave the organisation a structured approach to important information security issues that had to be thought through. The *implementation of best practice* per se was seen as an important reason but not as major a driver as the users of the Standard of Good Practice for Information Security (ISFSTD 2006) saw it. In addition, reasons for choosing ISO/IEC 17799 (2005) were that the *system can be certified* and the standard itself has a *good public name*. For example, one interviewee chose between ISF (2006) and ISO/IEC 17799 (2005) based on the certification option:

R: "...ISF was one of the references. There were good checking lists but ISF cannot be certified...at the moment there is no other generic (than ISO 17799) standard that can be certified." (R2)

In this particular case the organisation used some of the ISF (2006) checklists when they were creating their information security management system. Two of the interviewees argued that the ISO/IEC 17799 (2005) standard offers a *risk-based approach to information security* while two others saw that the standard gave them tools for *risk management*:

R: "...we got evaluation parameters instead of guessing the current situation of information security." (R3)

So the standard was a measuring tool for the organisation in addition to the risk management tool. The interviewees recognised that there are better tools for risk management than the ISO/IEC 17799 (2005) standard, but they felt it also aided the risk management. Two of the interviewees perceived that the standard improves the *overall quality* and one interviewee stated that the standard *supports and presents quality externally*. This was seen as an additional asset of the standard. Furthermore, *compliance with internal policy* was mentioned by one participant since they had created one beforehand within the implementation of ISO 9000 (2000). *Meeting governmental requirements* was raised by one interviewee because their organisation had a lot of clients in that business sector. One of the interviewees found it important that the standard is *internationally known* since their clients are mainly abroad or international organisations. *Rise in the overall security level* was mentioned too. This standard was seen as a *driving force for security issues* by one of the interviewees. This particular interviewee also thought that the information security and safety issues should be combined under the same domain:

R: "...what bothers me is that we have security and information security...I would like to speak about whole security, where information security is a part of it." (R4)

Here the interviewee wanted to emphasize the roles of the security and information security domains and how they are related to each other. This particular interviewee was handling the security issues in the organisation and saw that the joint operation of these domains is mandatory in order to be effective. Management support during the building phase of the ISMS was estimated as adequate, even strong. This was reflected as approval of expenditures, active participation in meetings, and creation of an information security policy that demanded effort from management and as spurring on those situations where daily routines almost overcome the development effort. These findings are presented in Table 2.

Table 2: Positive findings of management support

How the management support was visible	
+	Approval of expenditures.
+	Participation in meetings.
+	Creation of an information security policy that demanded effort from management.
+	Spurring.

Negative Findings of the ISO/IEC 17799 Framework

Thinking about the disadvantages, the interviewees foremost mentioned the expenditure. Thus, contrary to the perceptions of the users of the Standard of Good Practice for Information Security (ISFSTD 2006), the small and medium-sized enterprises view of the cost level was raised. These downsides, as expressed by the interviewees, are presented in Table 3.

Table 3: Downsides of ISO/IEC 17799 (2005) from the small and medium-sized enterprises' point of view

Reason	Mentions
Costs	3
Requires a lot of work	2
Coverage of corporate security	2
Hard to implement	2
Lack of implementation guidance	2
Readability of the standard	1
Does not cover project risks	1
Lack of references	1
Not known enough domestically	1
Does not ensure the actual quality of service	1
Value of the implementation is not visible right away	1
The creativity and business agility might be harmed	1

According to the interviewees, the implementation of the standard meant *costs* and *required a lot of work*. In the beginning, the work processes were changed and a lot of documentation was made because of the standard's requirements. The amount of work was even seen as back-breaking:

R: "... at the beginning ... heavy processes ... back-breaking documentation." (R1)

Not all the documentation was seen as necessary. Some of the documents were seen as only for fulfilling the needs of the standard, for example one interviewee thought the Statement of the Applicability was vain. The interviewee also thought they have not captured the essentials of the standard and have tried to build too heavy processes within a small organisation. The *coverage of other corporate security issues* was seen as a downside by two of the respondents. They perceived that the standard focused on information security but there were no interfaces to other corporate security issues:

R: "To the security of the foreign affairs the standard does not touch at all ... and some parts are only partially covered ... for example the fire safety, the standard is taking these quite easily, there's a mention in some subordinate clause." (R2)

The ISO/IEC 17799 standard was also seen as *hard to implement*. The segregation of duties proved to be very hard due to the lack of the resources:

R: "... segregation of duties ... we were a much smaller organisation at that time ... in lot of places was my name." (R5)

This was perceived as problematic, especially when the implementing organisation is a small one. Certain duties have to be integrated for efficacy reasons and lack of resources; on the other hand, the standard demands that some duties are segregated. Furthermore, two of the interviewees raised the isolation of loading areas as hard to implement as they were software companies. One of the organisations had no loading area at all, and the other had one in their premises but it was not used at all. One also commented on contingency plan issues and correct processing in systems:

R: "Implementing the standard is different than in big organisations ... can an SME do a thorough contingency plan and test it with reasonable resources ... correct processing in all systems? ... who would test the security of the e-mail system? ... for example routers, can we get the source code for evaluation?" (R2)

These are examples where a generic standard cannot give proper guidance on the implementation of the standard. The implementation could have been easier if there had not been a *lack of implementation guidance*, and the *readability of the standard* was low:

R: "It took a long time to really understand the requirements ... how to read the standard ... how to implement it." (R4)

The readability was not related to the English language; rather, it was the content of the standard that was not so easy to understand. One interviewee mentioned that the standard is not suitable as a stand-alone Risk Management tool as the standard *does not cover project risks*:

R: "... (17799) was not a sufficient tool for risk management alone ... does not cover project risks ... (in our company) we did not think about what could cause delays to the project, what effects it could have on financials and business. " (R1)

This interviewee recognised that the standard is not a primary tool for Risk Management and there are better ones available. But the interviewee wanted to highlight that the standard is not suitable for covering the project risks as is. The *lack of references* got criticism:

R: "There are no references in the standard where there are pointers to academic research ... you have to trust that the current practices on which the standard is based are good." (R2)

This particular interviewee’s organisation had started their implementation project by analysing some academic research on standards. They found there were no pointers to academic research in the ISO/IEC 17799 (2005) standard. One of the interviewees perceived that the standard *is not known domestically*. On the other hand, this organisation was more concentrating on the international markets where the standard was seen as well known. One of the interviewees was wondering about the value of the certification itself as the certificate *does not ensure the quality of service*; the organisation can achieve the certificate if its processes are defined and they are followed promptly, and this could end up in the situation described below:

R: "... (the standard) does not guarantee the result ... we can produce bad service with good information security." (R3)

This particular interviewee was worried about producing a bad or incorrect service. They measured client satisfaction with surveys. But as one other interviewee mentioned, measuring is reactive in nature and faults may happen. The problem is that the faults might be detected afterwards and the result could be a dissatisfied client. One finding was that the *value of the implementation is not visible right away*. The information security officer and management had doubts as there were no visible results right away when parts of the standard were implemented. As an advantage, the standard provides a solid framework and structured way of working, but the disadvantage is that *the creativity and business agility might be harmed*:

R: "... (ISO is) a double-edged sword ... harms agility and creativity a bit ... on the other hand, keeps the chaos away." (R3)

This particular interviewee stated that it is better to have this kind of situation because in the long run it is more important to keep the chaos away. The creativity is of course important for a software company, and agility can be seen as a competitive advantage in small and medium-sized organisations. Other negative issues were related to interactions with the management. One of the interviewees mentioned that a technical sparring partner was missing and one mentioned that some of the work had to done off the record because the management did not allocate enough resources for the work. One interviewee said that the management’s participation in meetings hindered open discussion of problems. The latter is reflected in the following quote:

R: "... if we need to discuss openly, people might shut up so that the management won’t hear unpleasant issues." (R2)

Open discussions are needed for capturing the personnel’s development ideas and problems they have perceived,. But if the personnel have fears about the possible consequences of raising problems, they will not be open in that sense. The comment above reflects a tricky situation: the management’s visible commitment is needed, but it may also have downsides. These views are gathered in Table 4.

Table 4: Management’s lack of support for information security management system work

Downsides of the management’s support
– No sparring partner on technical issues.
– Some of the work had to done off the record.
– Management’s participation in meetings hindered open discussion of problems.

Discussion

As far as the author of this study knows, there is no empirical research available on the implementation process and results on putting the ISO/IEC 17799 (2005) standard into practice in organisations. This study aimed to fill this gap in the research by exploring how the practitioners perceive the ISO/IEC 17799 (2005) standard as an information security management framework. This study is important as it reveals novel information on implementation of the ISO/IEC 17799 (2005) standard.

Limitations of the Study and the Validation Criteria

This study has some limitations. The sample was quite small, four Finnish small and medium-sized organisations and five interviewed persons, so these findings might not be fully generalized. A larger sample with both domestic and international organisations could reveal more information on these issues. Furthermore, as the study focused on information security managers and their views on the standard, the study lacks the view of the management and the personnel. To give the big picture, the views of the regulators and the system auditors are needed.

The Klein and Myers (1999) criteria were used as the validation criteria. Accordingly, the validation of this research is as follows. *The principle of Contextualization*: the interviewees were asked to recollect the context and the facts surrounding the events that led to the development of their information security management system. *The principle of Interaction between the Researchers and the Subjects*: the interviews were semi-structured in nature and open questions were used, so the interviewees were allowed to provide their own interpretations of the events. *The principle of Abstraction and Generalisation*: this principle was followed by abstracting the interpretations of the cases and arguing from the particular to the general, and purposive sampling was used. *The principle of Dialogical Reasoning*: the narrative section was evolved through iterations and internal reviews. *The principle of Multiple Interpretations*: this research aimed at understanding the relationships between context and intentions, whereas power issues were not studied and social actions were in a minor role in the four organisations studied, and *the principle of Suspicion*: the data collection consisted of five interviews and four organisations, thus reducing the possible bias of one interview; control questions were used in the interviews and internal reviews were used to validate the interpretations.

Discussion of the Results

Based on the answers from the interviewees, the small and medium-sized organisations are mostly interested in responding to pressure from clients. The information security management system creates business and gives support to the organisations’ sales efforts, which is how the management support is ensured. Contrary to the view of larger organisations (ISFSTD 2006), the management system itself was seen as cost, but the certification of the information security management system was still deemed a worthwhile investment. The interviewees perceived the image of ISO/IEC 17799 (2005) as good, and it helped in the choosing the standard. Furthermore, the interviewees estimated that the information security system raises the overall quality of the organisation, a factor that heightens management support. The certification itself was seen as an asset; it could be utilised in many ways, from external marketing to showing the organisation’s own personnel the management commitment to information security. Figure 1 depicts the factors and outcomes of the information security management system based on ISO/IEC 17799 (2005).

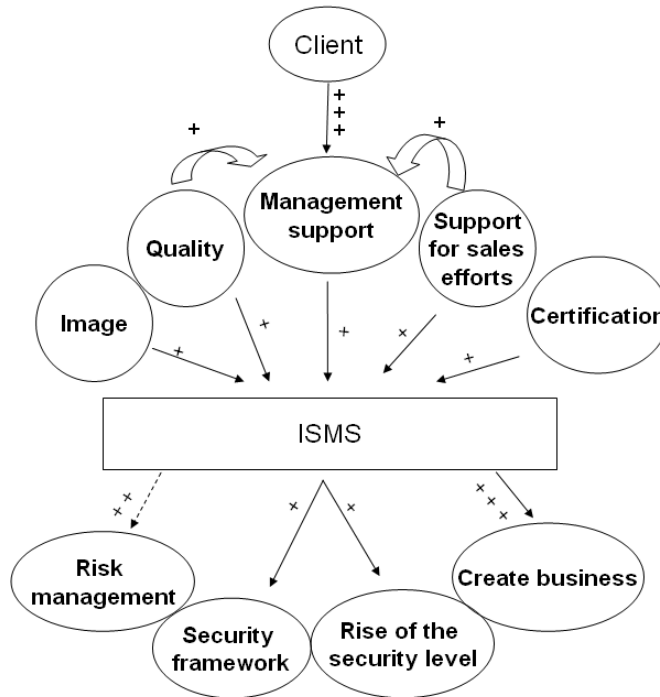


Figure 1: Factors affecting the implementation of the ISO/IEC 17799 (2005) standard and how the system affected the organisation

Even though some criticism was raised, these practitioners evaluated the ISO/IEC 17799 (2005) standard as offering a trustworthy security framework. It offers a risk-based approach to information security and could be utilised in risk management, even though the standard is not a dedicated tool for handling risks. The information security understanding increased among all personnel groups during the implementation of the standard, as did the overall security level. One should keep a keen eye on the starting level of the management, which was deemed low by three of the interviewees. Is it that the management is too focused on business and don't see the importance of information security? What would the consequences of a major information security breach be in a small or medium-sized organisation? Could it survive and continue its operations like a larger organisation could due its larger resources? Where do we stand regarding the information security? These kinds of questions should be asked among the management within the small and medium-sized organisations because the client organisations, or at least those that are sensitive to information security, are asking their subcontractors and business partners.

Furthermore, the implementation of the ISO/IEC 17799 (2005) standard heightened the understanding of information security in all personnel groups and the security understanding broadened from technical security to information security management and corporate security. For example, it was hard to segregate the duties within these small or medium-sized organisations because of the small numbers of personnel. As a result, the segregation of duties would not act as the control it was meant to be. The benefit of the standard in this case is that it pushes the organisations to clarify the processes and make better documentation. Thus the risks related to assets, whether people (losing key personnel or frauds) or data (forgeries), are diminished. The standard gives guidelines on how to protect sensitive information, yet leaves a lot of room for the actual implementation of the controls. The interviewees also perceived that the implementation of the standard changed the whole way of working towards a more secure way of practising it. This means that the client actually benefits from the implementation of the standard too. And, according to the interviewees, these small and medium-sized organisations gained from the new information security processes as well. Ideally, this new and good work practice is incorporated in day-to-day actions. This of course calls for continuous management support. The management support is also needed for guaranteeing the successful implementation of the process, as validated in the literature (von Solms & von Solms, 2004; Björk, 2006). The ISO/IEC 17799 (2005) standard itself emphasises a continuous improvement process, which forces organisations to always think about security and the risks involved in doing business.

The interviewees mentioned that they used the ISO/IEC 17799 (2005) standard as a source when making their information security management system and the information security policy. Baskerville and Siponen (2002, 338) have stated that using generic standards as a basis for security policy development has several shortcomings. They listed four cases: 1) generic standards do not pay adequate attention to the fact that organizations differ, and therefore their security requirements will differ; 2) generic standards do not take into account the social nature of the problems; 3) generic standards overlook the normal business requirements of organizations and as a result a conflict between the organization's normal business requirements and security requirements proposed by security standards may arise; and 4) generic standards are broadly written necessitating ad hoc managerial decision making and judgment. Baskerville and Siponen (2002, 338) also expressed the opinion that the generic standards do not provide any help concerning these decision-making problems.

Two interviewees mentioned that the ISO/IEC 17799 (2005) standard does not adequately cover the corporate safety issues and there is no link to them. This is a good point; the information security cannot be an isolated system. It has to be connected to other safety-related issues: personnel management, environmental risks, fire safety and so on. Furthermore, the interviewees estimated that typically the biggest lack of security was on the soft side - human or process-related issues - whereas the technical issues were typically in good shape before the implementation of the standard. Dhillon and Backhouse (2000) have stated that computer security in itself is not a technical problem; it has social and organizational dimensions that involve people who operate the technical systems. They suggest that information security principles need to be expanded to incorporate responsibility, integrity of people, trustworthiness and ethics to the classic CIA triad model. Furthermore, they state that information security should not simply be viewed as means of protecting physical assets alone. By taking individuals and their social relationships into account, the protection level should be expanded (Dhillon & Backhouse, 2001). There was some criticism of the fact that the ISO/IEC 17799 (2005) standard is not academically analysed. Furthermore, the trustworthiness of the standard itself is an issue. ISO/IEC 17799 (2005) certification can give organisations or their interest groups a false sense of security as management or third parties could associate the "certified" or "compliant" status to mean a secure system on which no further action needs to be done.

A lot of criticism was raised on the readability of the standard. The interviewees found some parts of the standard difficult to implement and gave some ideas for the improvement of the standard. As one can see, the guidelines given in the ISO/IEC 17799 (2005) standard are multifaceted. For example, on auditing, the standard demands clock synchronisation as the correct setting of computer clocks is important to ensure the accuracy of audit logs

(ISO/IEC 17799 2005, clause 10.10.6). The person who is going to perform log audits might see confidential information; thus non-disclosure agreements are needed (ISO/IEC 17799 2005, clause 6.1.5). There should also be controls to safeguard operational systems and audit tools during information systems audits (ISO/IEC 17799 2005, clause 15.3.2). On segregation of duties, the ISO/IEC 17799 (2005) standard states: "10.1.3 describes how duties may be segregated to prevent fraud and error. It may not be possible for smaller organizations to segregate all duties and other ways of achieving the same control objective may be necessary." All these examples show that the standard is not easy to implement.

The new ISO/IEC 17799 (2005) standard is not strict on the implementation of the controls, as the following excerpt shows: "This code of practice may be regarded as a starting point for developing organization specific guidelines." and it continues: "Not all of the controls and guidance in this code of practice may be applicable." (ISO/IEC 17799 2005, 11). The ISO/IEC 17799 (2005) standard leaves room for organisations' own guidelines and controls by stating: "Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners." (ISO/IEC 17799 2005, 11). These are good intentions but are they acting as solid guidelines? The small and medium-sized organisations proposed that the ISO organisation could make guidelines and mappings of the safety functions as a starting point.

All these reflect that there is a need for a more agile framework for implementing the ISO/IEC 17799 (2005) standard in practice. Perhaps by combining the agile methods with the development of the information security management system we could have a new approach to the actual information security management work?

Conclusions

Information security is a necessity for all organizations, no matter what the size or industrial sector. To cover the vast variety of risks involved in modern businesses, we need both technical and administrative information security; thus the need for information security management is quite clear. Especially for small and medium-sized enterprises, development of an information security management system based on ISO/IEC 17799 is a big effort. The development process itself can be a project starting from initialisation of the risk analysis and the main goal can be the certification of the system. But in order to be successful, the information security work itself has to be implemented in the daily activities of the organisation. The information security understanding and the continuous support of the management are crucial.

Although there are some deficiencies in the ISO/IEC 17799 standard, the practitioners see the standard as valuable and worthwhile implementing as it gives the organisation an information security framework. Yet the standard is not a silver bullet to the information security problems. The readability of the standard was criticised, as was the difficulty of the implementation. It is important to understand that the standardisation is not necessarily needed for good information security management. And the certificate or standard itself does not guarantee the adequate information security level of an organisation.

This study aimed at analysing experiences of putting the ISO/IEC 17799 standard into practice. There are a lot to be studied though. It would be interesting to find out whether there any practices in use that are totally missing in the ISO/IEC 17799 standard? Furthermore, it would be interesting to find out how to combine agile methods and the development of an information security management system so that a tailor-made information security management system based on the actual risks of an organisation can be built. As one interviewee stated:

"Information security should not prevent the business; on the contrary, it should support it." (R2)

References

- Baskerville, R. & Siponen, M.T. 2002, 'An Information Security Meta-policy for Emergent Organizations' *Journal of Logistics Information Management, special issue on Information Security* vol. 5-6, pp. 337-346.
- Bishop, M. 2005, 'The insider problem revisited: The insider problem revisited' paper presented to workshop on New security paradigms NSPW '05.
- Björk, F. 2006, *Implementing Information Security Management Systems - An Empirical Study of Critical Success Factors*, viewed 7.9.2006 <<http://www.dsv.su.se/~bjorck/files/bjorck-thesis.pdf#search=%22security%20scandinavian%20style%22>>.
- Deloitte. 2005, *Information security research*, viewed 23.8.2006 <<http://www.deloitte.com/dtt/research/0,1015,sid=1013&cid=85452,00.html>>.

- Dhillon, G. & Backhouse, J. 2000, 'Information system security management in the new millennium' *Communications of the ACM* vol. 43, issue 7, pp. 125-128.
- Dhillon, G. & Backhouse, J. 2001, 'Current directions in IS security research: towards socio-organizational perspectives' *Information Systems Journal* vol. 11, issue 2, pp. 127-153.
- DTI. 2005, *The Empirical Economics of Standards* viewed 27.11.2006 <http://www.dti.gov.uk/files/file9655.pdf>.
- Eskola, J. & Suoranta, J. 2001, *Johdatus laadulliseen tutkimukseen*. (In Finnish). Vastapaino, Jyväskylä.
- Eskola, J. & Vastamäki, J. 2001, *Teemahaastattelu: opit ja opetukset*. (In Finnish) In: *Ikkunoita tutkimusmetodeihin I. Metodien valinta ja aineiston keruu: virikkeitä aloittelevalle tutkijalle*. PS-kustannus. Gummerus kirjapaino Oy, Jyväskylä.
- Ernst & Young. 2005, *Global Information Security survey 2005* viewed 23.8.2006 <http://int.sitestat.com/ernst-and-young/international/s?Global-Information-Security-survey-2005&ns_type=pdf>.
- Gerber, M. & von Solms, R. 2005, 'Management of risk in the information age' *Computers & Security* vol. 24, pp. 16-30.
- Hirsjärvi, S. & Hurme, H. 2000, *Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö*. (In Finnish). Yliopistopaino, Helsinki.
- Homeland. 2006, *The Department of Homeland Security, USA* viewed 24.8.2006 <<http://www.dhs.gov/dhspublic/>>.
- Im, G. P. & Baskerville, R. L. 2005, 'A longitudinal study of information system threat categories: the enduring problem of human error' *ACM SIGMIS Database* vol. 36, issue 4.
- ISF. 2006, *Information Security Forum* viewed 22.6.2006 <<http://www.securityforum.org/html/frameset.htm>>.
- ISFSTD. 2006, *Information Security Forum. The Standard of Good Practice for Information Security* viewed 25.8. <http://www.isfsecuritystandard.com/index_ns.htm>.
- ISO/IEC 9000. 2000, *ISO 9000-14000 standards* viewed 16.9.2006 <http://www.iso.org/iso/en/iso9000-14000/understand/selection_use/selection_use.html>.
- ISO/IEC 17799. 2005. *ISO/IEC 17799:2005(E) International Organization for Standardization. Information Technology — Security Techniques — Code of Practice for Information Security Management*. Geneva. ISO Copyright Office.
- Klein, H. K & Myers, M. D. 1999, 'A set of principles for conducting and evaluating interpretive field studies in information systems' *MIS Quarterly* vol. 23, issue 1, pp. 67-88.
- OECD. 2006. OECD Guidelines for the Security of Information Systems and Networks. [Web document.] Available: <http://www.oecd.org/dataoecd/16/22/15582260.pdf>. [Referenced 24.8.2006.]
- O'Connor, M. 2005, 'The implications of Sarbanes-Oxley for non-US IT departments' *Network Security* vol. 2005, issue 7, pp. 17-20.
- Pinder, P. 2006, 'Preparing Information Security for legal and regulatory compliance (Sarbanes–Oxley and Basel II)' *Information Security Technical Report* vol. 11, issue 1, pp. 32-38.
- Relyea, H. C. 2004, 'Homeland security and information sharing: Federal policy considerations' *Government Information Quarterly* vol. 21, issue 4, pp. 420-438.
- Schultz, E. E. 2004, 'Sarbanes–Oxley—a huge boon to information security' *Computers & Security* vol. 23, Issue 5, pp. 353-354.
- Shephard, B. 2002, 'Information security—who cares?' *Power System Management and Control Conference* Publication No. 488, 17-19 April 2002, pp.124 – 129.
- Siponen, M. T. 2005, 'Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods' *Information and Organization* vol. 15, issue 4, pp. 339 – 375.
- Siponen, M.T. 2006, 'Information Security Standards Focus on the Existence of Process, Not Its Content?' *Communications of the ACM* vol. 49, issue 8, pp. 97 – 100.
- von Solms, B. 2001, 'Information Security – A Multidimensional Discipline' *Computers & Security* vol. 20, pp. 504-508.

- von Solms, B. 2005, 'Information Security governance: COBIT or ISO 17799 or both?' *Computers & Security* vol. 24, pp. 99-104.
- von Solms, B. & von Solms R. 2004, 'The 10 deadly sins of information security management' *Computers & Security* vol. 23, issue 5, pp. 371-376.
- von Solms, R. 1999, 'Information security management: why standards are important' vol. 7, issue 1, pp. 50-58.
- Sutton, S. G. & Arnold V. 2005, 'The Sarbanes-Oxley Act and the changing role of the CIO and IT function' *Int. J. Business Information Systems* vol. 1, issues 1/2.
- Theoharidou, M., Kokolakis, S., Karyda M. & Kiountouzis, E. 2005, 'The insider threat to information systems and the effectiveness of ISO17799' *Computers & Security* vol. 24, pp. 472-484.
- Tong, C. K. S., Fung, K. H., Huang, H. Y. H. & Chan, K. K. 2003, 'Implementation of ISO17799 and BS7799 in picture archiving and communication system: local experience in implementation of BS7799 standard' *International Congress Series*.
- Whitman, M. E. 2003, 'Enemy at the gate: threats to information security' *Communications of the ACM* vol. 46, Issue 8.

Copyright

Timo Wiander © 2007. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.