Information Security Standards and Global Business

Jorma Kajava[1], Juhani Anttila[2], Rauno Varonen[3], Reijo Savola[4], Juha Röning[3]
University of Lapland[1], Quality Integration[2], University of Oulu[3], VTT Technical Research Centre of Finland[4]
Jorma.Kajava@ulapland.fi, Juhani.Anttila@telecon.fi, Rauno.Varonen@oulu.fi, Reijo.Savola@vtt.fi, Juha.Roning@oulu.fi

***Abstract*-Information security management is becoming an increasingly important concern in nowadays business co-operation. Information security issues, however, have a surprisingly dualistic nature: almost everyone seems to be somehow familiar with them, but very few have a deeper understanding. Due to its multifaceted nature, information security should not be regarded as a separate concern; it is deeply intertwined with a multitude of business and societal functions. Of particular interest here is the integration, or embedding of information security into real business processes. In this study, we investigate the significance of information security standards for global business. The role of information security management is analyzed against the changing global market situation. An information security management approach applying international standards supports companies and other organizations in carrying out their business and co-operation globally.**

I. Introduction

Günter Verheugen, Vice-President of the European Commission and European Commissar for Enterprise and Industry, stated in a recent interview that one of the most important standardization areas is information security. He went on to say that standardization is an integral part of the European Commission's policy to enhance the international competitiveness of European business, remove commercial barriers and enact better legislation. In general all standardization aims to bring with it the following benefits to all organizations:

- Improved product performance and quality
- Decreased operational costs
- Facilitation of better communication between humans and organizations

Information security is closely linked to basic societal structures and national defence. It also comprises a variety of pre-warning systems and the fight against organized international crime.

To European organizations, the global application of international standards in general and information security standards in particular is becoming increasingly significant owing to the transfer of industrial production to countries with low labour costs. These transfers include not only subcontracting work and technical tasks, but entire production lines. Even planning and design are being transferred to low-cost countries. Outsourcing means that even the production of services, such as help desk services, is no longer tied to a particular physical location.

II. Standardization for Information Security Management

Information security-related issues are assuming an increasingly important role in our society extensively. Information security, however, has a surprisingly dualistic nature. Almost everyone is somehow familiar with it, but very few have a deeper undestanding of the information security management. This may be because information security is multifaceted and involves aspects of technology, business processes, organizations and individual behaviour. Previously, most attention was focused on technology and information networks, but now individual, organizational and managerial issues have come increasingly to the fore. Due to its multifaceted nature, information security should not be regarded as a separate concern; it is deeply intertwined with a multitude of business-related and societal functions [6]. Of particular interest here is the integration, or embedding of information security into business processes.

From the viewpoint of information security management, standards offer important references. For a fairly long time, we have relied heavily on the British Code of Practice for Information Security Management [2], to the point that it has become the *de facto* standard within the IT community. Recent years have seen the emergence of the international standards, such as ISO/IEC 17799 [4] and ISO/IEC 27001 [5], for information security management.

Although the situation looks rather good as far as standards are concerned, we must bear in mind the dual nature of information security. We must ask, whether the mere existence of standards is enough to ensure information security, or whether a wider perspective should be adopted.

III. Information Security Management Creates New Challenges

Many organizations still regard information security as something that can be taken care of by the generous application of money and technology. Nonetheless, oiling the wheels of the organization is a critical part of success and often involves improvements in information security, too. However, this approach leaves central factors out of the equation: the

1-4244-0726-5/06/$20.00 '2006 IEEE

www.manaraa.com

individual employee and the business managers. People working in organizations are definitely the critical factor in the implementation of information security. On the other hand, enhanced security may also result in reduced privacy and a deteriation of the working atmosphere. And all managers should manage their organizations' business activities also in regard to information security among their other business duties.

Standards serve to define the main concepts, principles and components of information security management. However, we must never lose sight of the key factors: commitment of the senior management and organization-wide information security awareness.

Serious challenges are created when the standards are being applied in individual organizations that are gearing their activities toward the global market. These organizations are waking up to the old truth that although information security is an elementary everyday notion, it is simultaneously a multidimensional, convoluted phenomenon.

IV. Information Security And Outsourcing

Outsourcing of business activities and functions during the 1980s and 90s took place in an atmoshere of trust. A kiosk owner, for example, would take his ledgers to an acquitance's accountancy firm. Both parties of this transaction knew each other and an atmosphere of trust had been established long before the actual operations.

The current trend is to transfer goods production and even service provision to the care of unknown people and organizations situated in low-cost countries. How can trust be developed and nurtured in these circumstances?

During the mid-1990s, some members of our team participated in an industrial project focusing on studying and promoting information security in outsourcing ventures. The initial results were a little disconcerting. Quantity seemed to offer high efficiency, allowing the subscriber of services to transfer their best "brain potential" to the company's key functions.

This soon led to the notion that all activities that could be outsourced, should be outsourced. But that's not how it works. It took a little time to persuade the company management that outsourcing relies on establishing strict security procedures and standards, otherwise the company runs the risk of losing information security. To prevent that, any critical points must be identified and solved so as not to lose information, security and the quality of the contracted services.

If the parties in an outsourcing agreement are to profit from cooperation, the following preconditions must be satisfied:

- Both partners' IT capabilities must be at the level required by today's demanding business environment.
- Both partners' information security capabilities must be at a high level prior to cooperation.
- Both parties, particularly the external service provider, must agree on the information security requirements imposed by the collaboration.
- The agreement negotiations are an essential process and, if need be, the parties must utilize the services of external specialists to ensure success.
- Matters pertaining to the partners' strategic operations must be kept under the direct control of each company.
- All cooperation must be based on mutual trust.
- Cooperation will only succeed if both parties feel they have something to win by it (win-win principle).

In offshore oursourcing, a ready-made environment of trust is rarely in place, and even the cooperation partner may be faceless. Nonetheless, information technology capabilities tend to be similar in various countries and on different continents, because the same industry standards are in use all over.

However, in many places information security related solutions, although based on standards, are still relatively primitive. Only if it can be assumed that the external partner's managers and employees are familiar with the basics of information security, the situation is fairly good. But cultural norms, habits and values may differ greatly in different countries and on different continents. Information security is strongly a cultural issue. In Finland, for example, a non-disclosure clause will almost invariably be respected - which is far from the case in some other cultures.

An atmosphere of trust is essential for all business. That requires not only proper security guidelines and physical security, but also personal, equipment, network, systems, software and data security practices as well as functional security. The goal of information security is to protect information systems and the data in them, in order to ensure availability, integrity and confidentiality.

In the past, not enough attention was paid on managing information security. A case in point is provided by some the current authors' experiences [8]. A few years ago, we were involved in evaluating the information security knowledge of a medium-sized company's senior management. Our initial impression was that everything was in order, the persons in question had the necessary knowledge of information security issues and the motivation to succeed in implementation. Which was to be expected, for they were the very people who were actually in charge of organizing and managing information security. Nonetheless, basic general knowledge and emotional motivation are not enough, managers should also be knowledgeable on the practical management of information security in the entire organizational context. On closer inspection, it turned out that the managers' information security skills were hardly better than those of ordinary employees. However, we expected the suggested information security approach to be adopted along with appropriate measures to educate the workforce. A couple of months later, we were startled to learn that the company had outsourced its entire information technology services, including information security management.

www.manaraa.com

V. Information Security Management Calls for Innovations

Although it seems almost trite to say this, success tends to increase when the cooperating partners share similar views on information security management. If anything, experience has taught us that simple solutions usually work in information security, too. Unfortunately, conditions in today's complex world often call for solutions that cannot be applied across the board. As a result, innovative approaches are being sought.

Within the Finnish IT industry, rapid progress has been made due to the efficient utilization of innovations, open-minded production expansion and development work. Further inducements are provided by the prevailing atmosphere that encourages and fosters cooperation. Positive incentives should also be brought to bear on the information security area to facilitate the development of innovative solutions.

A central question in information technology is security management. Organizations are seeking solutions to problems as they perceive them, but the current trend of subcontracting production and design to low-cost countries exarcebates the problem. What are the problems on the other side of the globe and how do local cooperation partners view the situation are key concerns in this regard. A standard that is adopted by one company should be applicable to where-ever it finds a partner, be it Lithuania or China.

In the absence of a suitable standard, a consortium of British companies collected theit best practices and published them as "A Code of Practice for Information Security Management" [2]. This was already in 1993, and 10 years later that seed has grown into international standards, referred to as ISO/IEC 17799:2005 [4] and ISO/IEC 27001:2005 [5], the standard for information security management.

The international standards offer improvements particularly as regards best practices in information security. These include better management of security arrangements among business partners, subcontractors and service providers as well as improved handling of problems associated with portable devices, wireless technology and the Internet. ISO/IEC 17799 is probably the single most important standard for information security management. In a sense, it provides a common information security language that allows organizations to communicate on equal terms regardless of their geological or cultural location. Consistently with the standard ISO/IEC 17799, the international standardization committee has also created another standard ISO/IEC 27001:2005 [5] for information security requirements to be applied in contractual situations.

The basic purpose of the information security standardization was that a common security model based on a shared standard is to enable companies to carry out their business and cooperate globally. Consequently, when these companies initiate joint operations, they can make significant time savings, as a common standard obviates the need to define principles for information security management. All that is required, is that the companies agree on the standards, use them and really understand their contents.

VI. Integration of Information Security Management with Business management Using Recognized Managerial Models

The latest development in the international standardization of information security management emphasizes the seamless integration of information security management with general business management. Especially ISO/IEC 27001 recommends applying also to information security management the recognized managerial principles of the general management models according to the ISO 9000:2000 [3] standards. Two methodological frameworks, the PDCA Model (Plan – Do – Check – Act) and the Process Management Model, are of utmost importance in this context [1]. However, the way in which these models have been applied to the standardization of information security is inadequate, and therefore their application requires additionally fundamental and multidisciplinary background knowledge. It is assumed that these models and all the possibilities they offer are familiar also to information security experts. This is not the case at all.

To ensure information security, organizations should carry out a number of different measures aimed specifically at enhancing information security when planning, carrying out and checking business activities/results and reacting to different situations. To that end, organizations should perform corrective, preventive and improvement actions, and–should the need arise–be prepared to comprehensively reengineer their business processes. The international standards mentioned above contain information detailing methodological approaches to information security tasks. However, although the ISO/IEC 27001 standard explicitly refers to the PDCA model, its application is rather unsystematic and inexplicit for the purposes of information security management.

In order to incorporate information security issues into business activities, one should understand what phenomena within single business processes and between different processes are critical from the information security point of view. Next, one should consider relevant needs and expectations, define suitable performance indicators and set quantitative information security targets in accordance with normal, proven process management methodologies. A key management issue is to monitor these process performance indicators in real time and to initiate–if required–such necessary measures to prevent, correct or improve performance as defined by the PDCA model. For business processes, the above-mentioned standards provide only very general guidance for defining information security control methods [1].

A critical issue for business process performance within organizations are the activities and awareness of the individual employees and managers involved in the processes, particularly how they understand their roles and responsibilities in relation to information security. No conflict

www.manaraa.com

should exist between a person's activities within a business process and his/her internal mental process, as such conflicts may give rise to significant information security threats. Chances of preventing and resolving these conflicts in an effective manner depend greatly on the organization's social networking culture and its human resource management practices, including procedures for compensating and rewarding as well as incentives and recognition. Only some of these problems may be avoided by replacing human activities within business processes by automatic IT solutions.

VII. Discussion

Does the introduction of the ISO/IEC 17799 and ISO/IEC 27001 standards spell the end of the road for busting international cooperation barriers and for establishing inproved information security? Knowing the principles underlying the best practices that the standards are based on, one is rather doubtful whether standards of that type alone can solve the problems. Admittedly, "A Code of Practice for Information Security Management" has been the linchpin of information security management for a number of years. But a lot of criticism has been levelled at it and a number of shortcomings have been pointed out. As a result, something more innovative is needed. However, for the time being, the approach adopted in ISO/IEC 17799 and ISO/IEC 20001, in spite of it's weaknesses, is the only widely recognized standard basis for information security.

Apart from the lack of a failsafe standard, the complex nature of information security poses problems for international business cooperation. To solve the problems, some researchers and consultants have proposed ready-made technological or procedural solutions. The difficulty in their widespread application lies in the fact that information security is a convoluted, multifaceted phenomenon. Each information security related event is in a sense unique, partially because organizations in different countries differ widely in terms of technology, corporate culture, hardware-base, security awareness, etc.. Factors such as these have to be taken into account in information security management at the organizational level.

Many things have reached the end of their development cycle when they can be packaged, or standardized. To provide an example, artificial intelligence has turned from an abstruse field of study into mainstream information processing. Correspondingly, e-learning is rapidly becoming an integral part of education, and there is no longer a need to emphasize specific aspects of the new learning environment. In terms of information security, we are used to small advances occurring as a response to experienced threats, but we should also be prepared to make a giant leap when the opportunity presents itself. Although the situation is under control in the sense that practical, ready-made solutions are currently available, the field is only opening up. Once we understand this and the challenges we must face and take action to overcome them, we will be at the forefront of information security. But pushing our way to the front requires innovative approaches both to current and future problems.

A particularly challenging - and rewarding - task in this undertaking will be the standardization of information security management. What complicates matters is that the situation looks different from the viewpoint of technical standards and that of managerial standards:

- **Technical standards:** The *interoperability* of different systems can only be achieved by means of standards. Major communications solutions, for example, can only be based on a common standard.
- **Managerial standards:** Standards *serve to improve business performance*. If the standards only fix the best practices, i.e., approaches that have already been tried in practice, and require their application, then they hinder the development on the never ending road towards excellent information security performance.

VIII. Proactive Progress in the Real World

In October 2005, Finland hosted a seminar in which TEKES, Finnish Funding Agency for Technology and Innovation, presented new initiatives planned for the near-future [7]. Of these, the GIGA project on converging networks, led by Mr. Kari Markus, offered an interesting connection to information security. The core of his talk, through the ears of an information security specialist, emphasized the following areas:

- International cooperation
- Common standards
- Information security

Thus, security experts are not alone in dealing with these issues. They are an inherent part of tomorrow's world. This realization soon leads to another: to be able to operate in the global market, countries such as Finland must take an active role in solving these issues. In this undertaking, it is not enough to look back and provide solutions that just meet current needs. A standard that fulfils present requirements is great, but a proactive approach would produce even better results for the future. But predicting the future is notoriously hard, because no one knows for certain what will happen, and there will always be surprises. One important area of information security management is the management of related risks.

Although international information security management standards are a novel thing, information security permeates the entire modern society. And it is not a challenge just in the developed countries, but all over the world. This is illustrated by difficulties experienced by companies who have transferred some or all of their production and even design to low-cost countries. Standards are required to facilitate the interoperability of information systems and of collaborating organizations and people. With the advent of ubiquitous

www.manaraa.com

computing, international standards and their innovative application will play an even greater role in our everyday lives.

IX CONCLUSIONS

Our studies and experiences prove that international standards of information security management are significant references for global business but their application cannot be done without a deep knowledge on modern business environments and sound business management practices and fundamentals of the information security and its managing difficulties and possibilities. Both managerial and technical standards are needed to support realization of information security in the international markets.

Information security is a multifaceted and multidisciplinary issue and it depends strongly on the cultural environment. International standards of information security are fairly new but they have a long historical background and have been used in many different kinds of organizations. However, business situations have radically changed due to networking of organizations and extensive global outsourcing of business activities and functions even from far away countries. In addition, significance of information has been increased in business transactions and immaterial services are essential parts of products. These aspects cause additional difficulties in applying the standards that are mainly based on experiences from more traditional business environments.

Senior executives are responsible of managing information security in organizations – but employees should be aware how to apply professional security practices in their everyday work. Executives have also the responsibility to develop organizational practices in their organizations for the future competitiveness. This responsibility particularly requires business integration and applying an innovative approach.

REFERENCES

[1] Anttila J. General Managerial Tools for Business-Integrated Information Security Management, 2006. URL http://www.qualityintegration.biz/InformSecPDCA.html

[2] British Standard 7799-2. Information Security Management Systems – Specification with Guidance for Use. Part 2. British Standards Institution, London, 2002.

[3] ISO 9000/9001/9004. Quality Management Systems, ISO, Geneva, 2000.

[4] ISO/IEC 17799. Information Technology – Security Techniques - Code of Practice for Information Security Management, ISO, Geneva , 2005.

[5] ISO/IEC 27001. Information Technology - Security Techniques - Information Security Management Systems - Requirements, ISO, Geneva, 2005.

[6] OECD Organisation for Economic Co-operation and Development. OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security. OECD Publications, Paris, France, 2002. 29 p.

[7] TEKES Finnish Funding Agency for Technology and Innovation. GIGA – Converging Networks 2005-2010, 2005. URL http://www.tekes.fi/giga/

[8] Kajava J, Anttila J, Varonen R, Savola R, Röning J, Senior Executives Commitment to Information Security – from Motivation to Responsibility, Computational Intelligence and Security CIS2006, Guangzhou, China 2006

www.manaraa.com