# Challenges for the comprehensive and integrated information security management

Juhani Anttila
International Academy for Quality (IAQ)
Helsinki, Finland / Milwaukee, USA (Admin.)
juhani.anttila@telecon.fi

Kari Jussila
Faculty of Pharmacy, University of Helsinki
Helsinki, Finland
kari.jussila@aalto.

***Abstract*—Information security management needs to be considered from the perspective of individuals, organizations and the society as a whole. The current situation is not satisfactory with regard to the concepts or practices and is becoming more challenging in the future. Further research and development of the managerial methodologies and practices are necessary for the needs of the new business environments, SMEs and startups. This our research focuses on the comprehensive and multi-disciplinary framework that aims at providing challenges for the new assorted research initiatives and innovations, and insight and guidance for the implementers who integrate the information security solutions within the management of business systems and processes together with other specialized managerial viewpoints. At present, the studies and practical implementations are very scattered and separate from each other, and difficult to be reconciled. Also effective collaboration of the administrative authorities, business leaders and security specialists, and effective links between the managerial, human and technical viewpoints are emphasized.**

***Keywords-information security; privacy; cyber security; management; research framework; business integration***

## I. INTRODUCTION

In practice, information security applies to the privacy data of individuals (personally identifiable information, PII), business sensitive information of organizations and information within the complex responsive cyberspace processes of the society. These areas of interest involve very different phenomena that however are much interrelated. In all these situations the responsibilities of different organizations are crucial. However, ultimately the human aspects have the most important role in perceiving and realizing security [1,2] and also in causing uncertainty and insecurity [3]. This applies to the ordinary people and business leaders and operators. The constructions of the human thinking processes [4], including theoretical concepts and models, rules and practices, and technological, managerial and social solutions, have a strong influence on how the situation is perceived, recognized, managed, evaluated and developed. Also all ICT solutions are constructions of the human mind.

The figure 1 is our general research framework for explicating all the related areas for considering information security in research and practice in a comprehensive way. Such an approach has become more necessary because of the large scale changes in the organizational and societal functions as the influence of the new advanced technologies, which have been characterized as the 4th industrial revolution, smart cities or industry 4.0 [5,10,11].

We have recognized that at present information security management is fragmented and conceptually unclear. Information security, privacy and cyber security are considered separately from each other. Additionally the technical and organizational/managerial perspectives are far apart. Human or social aspects are not sufficiently regarded.

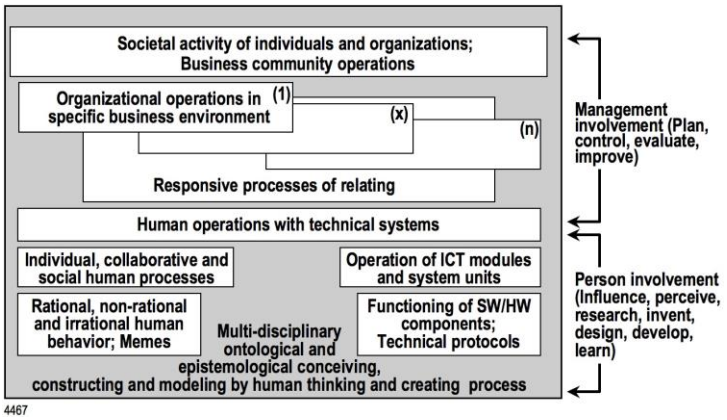


Figure 1. A comprehensive research framework for the information security management. Human phenomena come out through the individual people, society members, organizational members, business leaders, experts and researchers.

## II. CHALLENGES TO THE PRACTICAL INFORMATION SECURITY MANAGEMENT

Information security is a broad and multi-dimensional concept, including privacy [8], information security [7] and cyber security [9]. Unfortunately in practice and even in the international standards, we have recognized problems of incompatibility and ambiguousness in the concepts and their relationships, which hampers the adoption of these concepts and cause confusion in practical implementations. Consistency and compatibility between everyday and professional language of security is important, too. This also relate to the general meanings of the words 'information' and 'security', which are used by many different disciplines.

International standardization has the significant role in harmonizing professional thinking and practices. Especially we refer to the general international standards of the ISO/IEC JTC1/SC 27, which are well-known and used for the information security management everywhere in the world. This standardization also has a special role in setting requirements and giving guidance for the security

implementations, disseminating research results to practice and provoking new innovations.

The general standardization has always weaknesses and shortcomings due to the standardization process [12]. Hence, the organizations have their own responsibility to take the advantage of the science, technology, and experience in applying the standards, and the business leaders and experts should clarify, correct and complete general standards and find creative solutions in order to achieve business benefits in their implementations. In this context the organizations should take advantage also of the de facto, regional national (for instance [13]) and sector specific standards and relevant research reports (for instance [14]).

We have analyzed in our research the valid standard ISO/IEC 27001:2013 [7] from the user organization's point of view. The standard includes problem areas that are difficult to identify if one has not been involved in the standardization process or has not enough awareness of the business management or information security principles. We have commented these issues during the drafting process of the standard, but due to the consensus practice the comments were not taken into account. However, improvements can be made by the organizations themselves during the implementation. We present the following examples (chapters and clauses refer to table I):

1. The allocation of the risk processing items in the standard is confusingly unclear from the practical application point of view. In organizational practice it is natural to take the risk topics into account in a consistent way in planning (chapter 6), operation (chapter 8) and support (chapter 7).

2. Use of the controls for the risk treatment (clause 6.1.3) is expressed in a very complicated way although the issue is simple; the organization shall itself select the necessary controls from any source and design them according to their needs, and provide relevant documented information. Annex A of the standard is only a source of the possible controls. However, the organization is required to compare and justify the selected controls only against the controls presented in the Annex A. It is also unclear when such comparative measures should be taken. We have seen in practice that the the Annex A has not been understood in a correct way.

3. Statement of applicability (SoA) causes an unreasonable amount of work for organizations, when it refers to all of the items in the Annex A. The SoA is a 'How' issue and should not be included as a requirement. The standard should consider only 'What' issues.

4. The standard does not sufficiently support the organizations' business process approach. Nowadays the management of organizations is strongly based on the management of the business processes. Also practical risk management activities should be integrated with the management of the business processes [17].

In the professional practice, security management refers to coordinated activities to direct and control an organization with regard to security. A lot of security management methodologies have been developed and standardized. However, the organizations implementing the information security management are very different, and hence also the practical solutions must be different. For instance, information security is an especially important issue for SMEs and startups, which are driven by the dynamic changes through continual learning and agility with their limited resources. More than 99% of all the organizations are SMEs [24], for instance in Europe more than 22 million SMEs. However, established information security management methodology is not available for these business environments. The international standards are mainly based on the situation of the well-established organizations, which usually are large organizations. The standards could be useful for small organizations, if they had been drawn up in accordance with their circumstances. At present the standards are too complicated for SMEs and in particular for startups. Hence, a lot of research is needed in this area.

TABLE I. HARMONIZED STRUCTURE AND THE STANDARD CHAPTERS OF ALL THE ISO/IEC MANAGEMENT SYSTEM STANDARDS (IN ISO/IEC 27001:2013 XXX = INFORMATION SECURITY) [18]

| |
|---|
| 1.–3. Introductory issues |
| 4. Context of the organization |
| 4.1 Understanding of the organization and its context |
| 4.2 Understanding the needs and expectations of interested parties |
| 4.3 Determining the scope of the XXX management system |
| 4.4 The XXX management system |
| 5. Leadership |
| 5.1 Leadership and commitment |
| 5.2 Policy |
| 5.3 Organizational roles, responsibilities, and authorities |
| 6. Planning |
| 6.1 Actions to address risks and opportunities |
| 6.2 XXX objectives and planning to achieve them |
| 7. Support |
| 7.1 Resources |
| 7.2 Competence |
| 7.3 Awareness |
| 7.4 Communication |
| 7.5 Documented information |
| 8. Operation |
| 8.1 Operational planning and control |
| 9. Performance evaluation |
| 9.1 Monitoring, measurement, analysis, and evaluation |
| 9.2 Internal audit |
| 9.3 Management review |
| 10. Improvement |
| 10.1 Nonconformity and corrective action |
| 10.2 Continual improvement |

Integration implies that information security is considered in connection with the real and practical human, organizational and societal operations. This requires that we clearly understand all the involved phenomena (figure 1) and concepts in a holistic way, and effectively realize the necessary measures and evaluate the development according to the specific needs and expectations for information security management and information security assurance.

In order to ensure preserving high quality of security in organizations, solving problems properly and quickly, responding to the risks and promoting improvements, organizations should take into account information security in the strategic management of the business systems and operational management of the business processes [17].

We have recognized that the general situation of the organizational information security is not satisfactory now. Especially the top management of the different organizations, including public institutions and private

companies, has in this context the central role and responsibility to demonstrate leadership and commitment with respect to the information security management [3]. For instance in many organizations, the implementation of the general standard requirement [7] of the information security management is superficial or realized by building separate management systems for information security or only considering information security as a technical issue. In practice we have experienced the management/expertise dilemma: Managers and experts are isolated and do not collaborate with each other (figure 2) that feeds the disintegration of security [3].

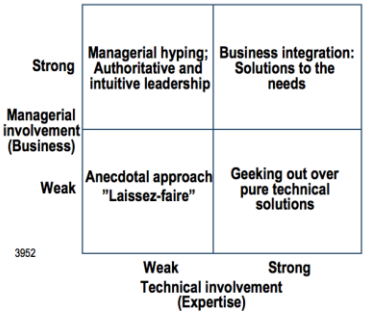


Figure 2. Organizational options for the solutions of the information security management. Our preference is the business driven integration based on continual learning.

The society as a whole is not any organization but a non-manageable 'scale-free' network of independent actors, consisting of individuals and institutions [15]. Although typically the authorities set big challenges [6] to the information security of the whole society, the societal development can only take place through diffusion from the development of the society members.

In the case of the human individuals, the security mainly depends on the individuals' own awareness, competence and attitude. In this context people should be considered as individuals and members of different organizations and societies. Also organizations are responsible to consider human privacy issues [16] seriously and responsibly.

Challenges of the information security can be met in practice through the strategic and operational management activities, professional expertise, research and development, innovation, statutory and regulatory requirements and the lifelong education and learning of the individuals.

## III. THE EXTENDED APPLICATION AREA AND SCOPE OF THE INFORMATION SECURITY MANAGEMENT

Today problems and reactive countermeasures against hostile actors are emphasized in the information security management and expertise. However, the fundamental meaning of security is positive (in Latin: sēcūrus - being without worry = sē- [prefix] - without + cūr(a) - worry + -us [adjective suffix]), and creative innovations should be directed for its continual improvement. This also means design activities for improving the dependability (reliability, maintainability and maintenance support) performance of the complex information dependent systems.

In addition to the security management, the requirement of integration also concerns many other related specialized managerial disciplines, including quality management, environmental management, human resource management, asset management, sustainability management, etc. Hence, we need a comprehensive approach to the implementation of all these disciplines within the organizations. The standardization bodies have defined the harmonized standard structure (table I) [18] that is used in all management system standards to help the organizations when they integrate the requirements of the different disciplines simultaneously into their businesses. Also the main information security standard ISO/IEC 27001 [7] follows this structure. From the managerial point of view, security aspects should be considered also with these other disciplines.

Items of the table I represent very typical and normal business management issues of any organization, which emphasizes the idea that information security management measures should be integrated with the normal business system, and separated information security management systems should be avoided in practical implementations.

## IV. RISK BASED INFORMATION SECURITY MANAGEMENT

All actors and activities of the society need information security and are influenced by the uncertainty of possible insecurity. This means that we are confronted with risks that means the effect of uncertainty on objectives [19]. In table II we summarize the categories of the information assets and risks related to the individual persons, organizations and the society and refer to the applicable general standards.

TABLE II. INFORMATION RELATED ASSETS, RISKS OF HUMAN INDIVIDUALS, ORGANIZATIONS AND THE SOCIETY, AND REFERENCE STANDARDS

| A person | An organization | A society |
|---|---|---|
| Privacy information risks | Business information risks | Collective information risks |
| An individual with a personal responsibility | An organization with the top management responsibility | A scale-free societal network of interlinked independent actors with nobody's or every actor's responsibility with its network impact capacity |
| • Information of personally direct or indirect what, where, how, etc.<br>• Personally identifiable information (PII) | • Business sensitive and crucial information in many forms, including digital or material form, or in the form of knowledge of people | • Information of large groups of actors<br>• Common mode information<br>• Critical infrastructure information |
| • No privacy management standards<br>• ISO/IEC 29100 series for guidance to organizations dealing with systems information, including communication systems or services<br>• The charters of fundamental rights<br>• Personal data protection regulation | • ISO/IEC 27001 and 27002 for requirements and guidance for organizational information security management | • ISO/IEC 27032 for guidance for providers and users of the services in the virtual and complex environment of the cyberspace on Internet |

4437

Effective risk management is the definite prerequisite for the effective information security management in the organizations. A great variety of methodologies is available, which has caused that in practice the situation is fragmented even at the conceptual level. Hence, a particular Risk Handling Library (RHL), based on the most relevant current ISO and IEC standards dealing with risk handling, is being considered by the information security experts. The organizational challenge is to find the appropriate means and integrate them seamlessly into the organizations' strategic and operational management processes in a creative way.

Risk management implies effective procedures of risk assessment and treatment, including appropriate controls [20]. In the organizational environments, the risk controls should be linked with the organizations' business targets and priorities. Business continuity management and contingency planning [21,22], recovery actions and resilience management [22] are closely related to the risk management.

Advanced organizations have implemented methodology by which their management is able measure the effectiveness of the organizations' internal control practice. With this approach the risk treatment recording can also improve the communication between the security specialists and senior management [23].

## V. CONCLUSIONS

In order to meet the challenges and to respond to the present and future needs, consistent further research and development are needed especially in the areas of the organizations' integrated information security management and the information security questions related to individual people and societies as a whole. Especially the impact of the phenomena of the 4th industrial revolution should be considered. A very topical research issue that we are currently examining and practicing is the information security management in startups combined with the IPR (Intellectual Property Rights) management. Also in this context the comprehensive research framework is useful.

We have considered the questions of information security conceptually and within practical business environments and referred to the related standardization. We are convinced that a sound theoretical foundation is a necessity for the sustained practical high quality security applications and the empirical studies in organizations in order to validate the applicable methodologies. Our comprehensive research framework has proved useful to provide a holistic understanding of the topic and clarify the relationships between the involved entities.

## REFERENCES


[1] J. Anttila, R. Savola, J. Kajava, J. Lindfors and J. Röning, "Fulfilling the needs for information security awareness and learning in information society". The Information Institute, The Annual Security Conference, Las Vegas USA, 2007.

[2] IBM, Reviewing a year of serious data breaches, major attacks and new vulnerabilities, Cyber security intelligence index, 2016. https://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03133usen/SEW03133USEN.PDF.

[3] J. Anttila, "Reinforcing business leaders' role in striving for information security". CIS Conference, Harbin China, 2007.

[4] K. Popper, "Three worlds", The Tanner lecture on human values, Delivered at the University of Michigan, April 7, 1978. http://tannerlectures.utah.edu/_documents/a-to-z/p/popper80.pdf.

[5] K. Schwab, "The Fourth Industrial Revolution: What it means, how to respond", World Economic Forum, 2016. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

[6] The European Parliament and the Council of the European Union, "Concerning measures to ensure a high common level of network and information security across the Union", Directive (EU) 2016/1148, 6 July 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

[7] ISO/IEC 27001:2013, Information security management, ISO, Geneva, Switzerland, 2013.

[8] ISO/IEC 29100:2011, Information technology - Security techniques - Privacy framework, ISO, Geneva, Switzerland, 2011.

[9] ISO/IEC 27032:2012, Information technology - Security techniques - Guidelines for cybersecurity, 2012.

[10] ISO/IEC JTC 1, Smart cities, ISO Geneva Switzerland, 2015. https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/smart_cities_report-jtc1.pdf.

[11] European Parliament, Directorate General for internal policies. Policy Department A. Economic and scientific polity. Industry 4.0, 2016.

[12] C. Paris, "Why ISO is in direct violation of World Trade Organization regulations", Apr 20, 2017, https://www.oxebridge.com/emma/why-iso-is-in-direct-violation-of-world-trade-organization-regulations/.

[13] M. Nieles, K. Dempsey and V. Yan Pillitteri, "An Introduction to Information Security", June 2017, NIST Special Publication 800-12 Revision 1, https://doi.org/10.6028/NIST.SP.800-12r1.

[14] R. Caralli, J. Stevens, L. Young and W. Wilson, "Introducing OCTAVE Allegro: Improving the information security risk assessment process", May 2007, Technical report CMU/SEI-2007-TR-012 ESC-TR-2007-012, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[15] (16) A. Barabási, Linked: How everything is connected to everything else and what it means for business, science, and everyday life. Plume Books. New York, 2003.

[16] The European Parliament and the Council of the European Union, "On he protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", 7 April 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[17] J. Anttila, J. Kajava, R. Varonen and G. Quirchmayr, "Business integrated information security management". In Lopez, J., Furnell, S., Katsikas, S., and Patel, A. (Eds.): Securing Information and Communication Systems: Principles, Technologies, and Applications. Chapter 3. Artech House. Boston|London, 2008.

[18] ISO/IEC, Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO, Annex SL, Proposals for management system standards, ISO, Geneva Switzerland. 2012.

[19] ISO, ISO 31000 Risk management - Principles and guidelines, ISO, Geneva Switzerland, 2009.

[20] ISO, ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management, ISO, Geneva Switzerland, 2011.

[21] ISO/IEC, 27002:2013 Information technology - Security techniques - Code of practice for information security controls, ISO, Geneva Switzerland, 2013.

[22] ISO/IEC, 27031:2011, Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity, ISO, Geneva Switzerland, 2011.

[23] D. Brewer and W. List, "Measuring the effectiveness of an internal control system", Gamma Secure Systems Limited, 2004.

[24] Eurostat, "Key figures on European business with a special feature on SMEs", 2011, http://ec.europa.eu/eurostat/documents/3930297/5967534/KS-ET-11-001-EN.PDF/81dfdd85-c028-41f9-bbf0-a9d8ef5134c5.