The 14 Layered Framework for Including Social and Organisational Aspects in Security Management

Y.Monfelt[1], S.Pilemalm[2], J.Hallberg[2] and L.Yngström[1]

[1]Department of Computer and Systems Sciences, Stockholm University, Sweden
[2]Division of Information Systems, Swedish Defence Research Agency, Sweden
e-mail: yngve.monfelt@dsv.su.se; sofie.pilemalm@foi.se; jonas.hallberg@foi.se; louise.yngstrom@dsv.su.se

Abstract

The ultimate aim of the COINS - COntrolled INformation Security – project is to investigate, assess, and provide tools to improve the information security status in organizations with a focus on public agencies. A central question for the project is how information security issues are communicated within the organizations, specifically underlining that communication is control in a cybernetic sense. The project is carried out in a number of steps embracing to design modelling techniques and metrics for information security issues in organizations (1), collect data from Swedish governmental agencies (2), use the modelling techniques to model communication of information security in organizations from different perspectives (3), to apply metrics on the data in order to assess information security levels in the agencies (4), identify gaps (5) and needs for improvement (6). The 14 layered framework, which is based on well established knowledge within information security: frameworks, models, standards, and terminology is presented. The scientific base is cybernetics, including variety engineering and recursion to provide adaptation and learning. The motivation for the research is that communication of information security issues within organizations tend to be insufficient and the mental connections between IT-security and information security work are weak, which prohibits the organization from learning and adapting in its security work. This is a report on research in progress.

Keywords

Information security management, holistic approach, applied research

1. Introduction

Adequately deployed information systems provide the means to increase the potential as well as the effectiveness and efficiency of business processes. However, the extensive use of Information Technology (IT) also comes with related security problems caused by the abstract nature of interacting systems – technical and organisational - and the seemingly lack of or inferior control of data or information. The obvious result is that the expected service - 'security' – is not produced with desirable quality. For assessing the technical systems' quality of security, assurance techniques are well established, such as the Common Criteria (CC, 2009). For assessing the information systems' quality of security, efforts to specify metrics based on, for instance, the ISO/IEC 27000 series are presently being taken.

The hereby presented research takes the holistic road towards analysing and constructing security metrics for information systems including their IT related components. The wholeness will weigh in technical and non-technical areas, using theories developed for open, adaptive, learning, feed-back systems as defined by system theoreticians such as Ashby (1963), Beer (1964, 1979, 1981), Boulding (1964), Ackoff (1976), von Bertalanffy (1956), Wiener (1948), Miller (1978), de Rosnay (1976), van Gigch (1974), and Checkland (1988). We are aware of current scientific demands for 'holistic' security which "...embraces the scientific method, new sources of objective data, and new perspectives from diverse fields from which new theories and approaches flow." (Shostack and Stewart, 2008, p.131), and will marry specifically cybernetics – the science of communication and control – with demands on modern organisations to produce high quality security services within their technical and organisational information systems.

The motivation for initiating this research was one of countless security reports (Swedish National Audit Office, 2007) stating, despite the Swedish public sector's initiative to prescribe the use of LIS – the Swedish version of the ISO/IEC 27001 – (International Standards Office, 2006) eleven government agencies were not considered to have reached adequate levels of information security.

To address needs of understanding, learning, controlling and managing information security, the COntrolled INformation Security (COINS) research project was coined. The ultimate aim is to investigate, assess, and provide tools to improve the information security status in organizations with a focus on Swedish public agencies. In this specific research a central question is how information security issues are communicated within the organizations, thereby specifically underlining that communication is control in a cybernetic sense. The research is carried out in a number of steps embracing to design modelling techniques and metrics for information security issues in organizations (1), collect data from Swedish governmental agencies (2), use the modelling techniques to model communication of information security in organizations from three different perspectives(3);

- ideally (according to available standards),
- formally (as stated in organizational available documents and policies) and,
- practically (as reported by respondents in selected agencies),

and to apply metrics on the data in order to assess the information security quality in the agencies (4) and identify gaps (5) and needs for improvement (6).

The research method applied can be expressed as applied general systems theory (van Gigch, 1974) combined with design science (Hevner et al. 2004).

This paper intends to give an overview of the design and test of the communication framework, its metrics and the syntax used. Finally it will give some tentative results based on empirical data. It is organized as follows: Firstly it explains the main characteristics of the 14 layered framework including how the test data were obtained through empirical investigations at an agency. The terminology used is

specifically commented before the preliminary findings and discussions are presented.

2. The framework for communication and control

The framework for communication and control was named The 14 Layered Framework. Its design is based on four high level characteristics: to facilitate communication between and within social and technical layers (1), to include strategic, tactic and operational decisions (2), to provide for communication mind-to-mind between executives and between technical means (3), and compactly, yet comprehensively, address the whole enterprise (4).

2.1. The 14 layers in communication

Information security depends on technical, as well as social and organizational aspects which together communicate and interact such that – in total – the organization steers and controls towards providing intended information security services with desired quality.

The technical flow of signals and their particular meaning in a specific message is standardized on seven layers in the ISO/IEC 7498-1 standard for Open Systems Interconnections (International Standards Office, 1998), while there are no standards or common understanding about the social and organizational layers or how these layers interact with the technical layers.

We present a fourteen layer framework, which adds seven social layers to the already existing seven technical layers. The construction of the seven social layers is partly founded on similar works presented by Kowalski (1994) as the Security By Consensus (SBC) model, the FRISCO report (Falkenberg et al., 1998) and also inspired by early works of Langefors (1968) on the meaning of information.

The framework is presented in Table 1, where two /generic/ communicating entities, A and B, are depicted on the top. Each one makes their own decisions (risk analyses considering desired security performance) based on their comprehension of Strength, Weakness, Opportunity, and Threat (SWOT) in their respective environments. In making decisions, A respectively B, considers what are the dependencies on social and organizational aspects concerning cultural, ethical and legal values and existing administrative and managerial issues. (This is typically a systemic question which is guided by the decision maker's knowledge, visions, etc, tied to the role and authority of the specific decision maker, and influenced by existing context.) The outcome of the respective SWOTs concerning the effect on the Quality of Service (QoS), i.e. the security performance, is communicated and decided between A and B. At the managerial level is expressed which information security was chosen for the particular issue – in the Table expressed as InfoSec (InfoQ). Since the thereafter preceding interpretation, at the organizational layer, will affect the implementation of how communication must be organized, it is expressed in the Table as Pragmatic meaning. The Semantic Message which can be understood by humans needs thereafter to be adapted to the technical levels.

The Table 1 can also be interpreted from below, where the seven technical layers add bits which have a standardized interpretation at each level according to the ISO/IEC standard 7498-1 (International Standards Office, 1998), and produce a data communication technology for a given application. Data needs to be adapted to provide a Semantic Message and Pragmatic meaning which can be used to produce sufficient technical and administrative information for dependable integrity. The legal, ethical and cultural aspects on the technical and administrative information security will further be blended in to produce the final decided effect.

Level	**Entity A**	**Peer-to-Peer Purpose**	**Entity B**
So14	SWOT	Effect	SWOT
So13	Cultural		Cultural
So12	Ethical		Ethical
So11	Legal		Legal
So10	Managerial	InfoSec(InfoQ)	Managerial
So 9	Organizational	Pragmatic meaning	Organizational
So 8	Adaptation	Semantic Message	Adaptation
Te 7	Application	DataQ	Application
Te 6	Presentation Coding	DataSec(Symbol)	Presentation Coding
Te 5	Session	Bits/Symbol	Session
Te 4	Transport	Protocol	Transport
Te 3	Network		Network
Te 2	Link		Link
Te 1	Physical Medium	Bits/s	Physical Medium

Table 1: The 14 layers in communication

In organizations, depending on authorizations and roles, decision makers appear on strategic, tactic and operational levels. The strategic decisions (EXE-0) concern the overall company policy and standards for management; the tactic decisions (EXE-1) concern the implementation of policy and standards on the managerial level while the operational decisions (EXE-2) concern the implementation of lower levels policies in the technical layers. While EXE-0 concerns and influences the whole organization, EXE-1 concerns and influences the Enterprise Communication Architecture (ECA) and EXE-2 concerns and influences the Data Communication Technology (DCT). Their respective systemic decisions are structured according to the Life Cycle concept (Plan-Do-Check-Act) applied from Avizienis et al. (2001) and Flood (1999). However, space limits makes it not possible to present this further here.

Acronym, name	Description
EXE, Enterprise eXecutive Entity	Executive processes motivate reasons for tasks and the policy of what to perform (QoS) and how (ECA) in relation to controlling the task through management and feedback
QoS, Quality of Service	An enterprise need to organize a structure for its QoS assets. For survival purposes, the Decision Motivator will strive for quality goals. QoS assets are assets of the enterprise which are accessed by roles authorized as trustworthy providers of security with respect to knowledge, needs and behavior. Humans in roles must be responsible, (accounted for their actions following the specific access).
ECA, Enterprise Communication Architecture	Humans in authorized roles are knowledge resources who give meaning to messages, for handling the social layers (7Sol), when establishing and communicating about the assets in relation to QoS
DCT, Data Communication Technology	Mechanistic resources, as technical layer applications, and administrative routines which support the ECA handling of social layer messages in communication.

Table 2: Legend of some central acronyms used in the 14 layer framework

3. Empirical investigations with an agency

At the agency, two investigations were undertaken; the formal communication of information security as expressed through policies and other internal documents (1), and the practice of information security as expressed through interviews with representatives on the three decision levels EXE-0, EXE-1 and EXE2 (2).

The structure for these investigations was based on the 14 layered framework, and organized for the interviews into eight themes: General information security work, Management information security work, Operative information security work, Information security needs, Problems and needs for change, Information security communication structures, Assessing information security, and Concepts and terminology.

Thus, we had data available both on how the agency planned to organize its InfoSec work and how it actually performed. These data, after analyses and compilations were compared to the ideal communication about InfoSec work expressed through the 14 layered framework. The next section explains shortly how this was conducted.

4. Terminology to obtain the ideal, planned and praxis of InfoSec

To address the problem of using a terminology related to information security which can be integrated into core business communication (and thus address the communication about the quality of the service 'information security') a reference model based on the normative security objectives in appendix A of the standard ISO/IEC 27001 (International Standards Office, 2006) was created. The construction of the terminology used in the reference model included, in addition to well known and established security standards and frameworks, specifically the FRISCO report (Falkenberg et al., 1998) which gives control perspectives on information systems in general. For each normative objective labeled A5-A15 in the standard, the number of occurrences of 229 selected security related terms was recorded. Based on this data

the fraction of occurrences was computed for each of the normative objectives. To analyze the information security work performed in an organization, statements representing the organization were classified as belonging to one of the A5-A15. Thereafter the number of occurrences of the 229 terms was counted for each of the statements and accumulated for all statements classified as belonging to the same A5–A15. Finally the fraction of occurrences was computed for each of the eleven A5–A15 sets of statements. The resulting distribution over A5–A15 was compared to the distribution for the appendix A of the standard. Figure 1 below presents the essence of how the terminology relates to the norm, and how test-statements (from the agency's policy documents) respectively test-responses (from the interviews at the agency with representatives of EXE-0, EXE-1 and EXE-2) are viewed.

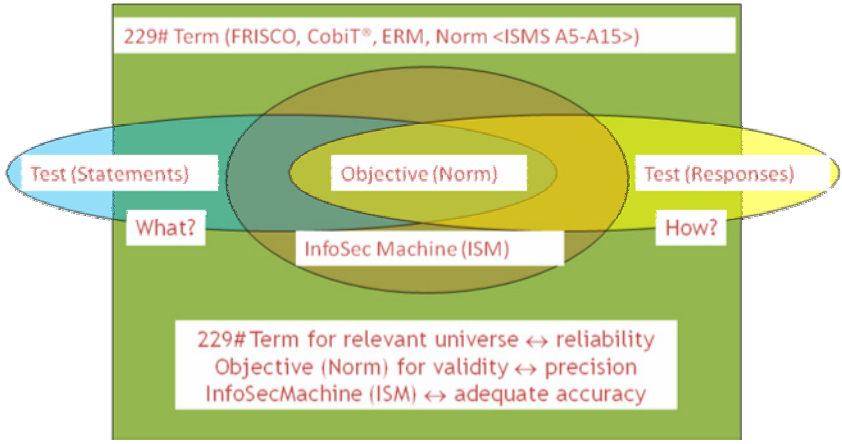

Figure 1: Reliability, precision and accuracy considerations for the analysis method, based mainly on the terminology and the 14 layer framework (Yngström et al., 2009a, figure 13)

Thus, the results from the calculations using the 229 selected security related terms may now be used to express and compare the ideal communication - the norm – with the policies – the agency's documents – and the practice of the agency – the interviews. This is presented in the following Figure 2-Figure 4.

Figure 2 presents the result from the analysis of the ISO/IEC 27001 appendix A with the normative objectives ordered by the number of occurrences of the 229 security related terms. This result should be considered the norm towards which the following analyses should be compared.

Figure 3 shows the results from the analysis of the studied agency documents as well as the norm. In the figure the label "Ch6" is a reference to chapter 6 of COINS Report #1 (Yngström et al., 2009a) where the full description of the analysis of the agency documents can be found. The objectives in the figure are presented in the same order as the norm in Figure 2 and shows how the relative distribution of the occurrences of the 229 security terms for the agency documents correlate with the norm.

Figure 4 shows the results from the analysis of the data from interviews with security personnel at the studied agency as well as the norm. The label "Ch7" is a reference to chapter 7 in COINS Report #1 (Yngström et al., 2009a). As with the analysis described above, the results are presented in same order as the norm. To support the interpretation of figures below, the understanding of norms/acronyms according to the standard is (including the consecutive numbering as applied in Appendix A of the standard):

Authorization (ATH) for ECA, A10
Accessibility (ACC), A11
Availability (ABY), A12
Account (ICI), A13
Account (QoS), A14
Account (LAW), A15
Policy (PCY), A5
Organization (ECA), A6
Asset (AST), A7
Cognition (COG), A8
Behaviour (BEH), A9

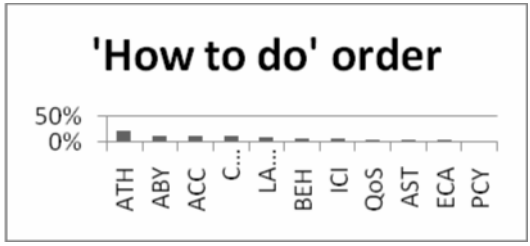

Figure 2: Relative occurrences of the terms for ISO/IEC 27001 appendix A

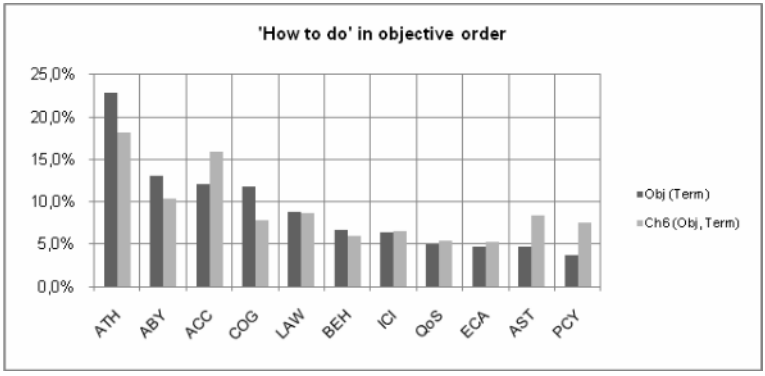

Figure 3: Relative occurrences of the terms from ISO/IEC 27001 appendix A and the agency documents

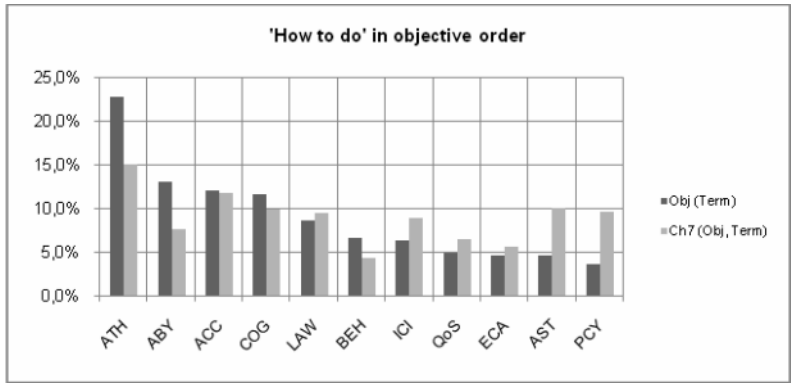

Figure 4: Relative occurrences of the terms from ISO/IEC appendix A and the interviews with agency personnel

5. Some preliminary findings from using the framework

In using the 14 layered framework including the reference terminology we were able to catch the communication about information security work within the agency in two ways; as planned according to the policies and as practiced according to the interviews. As it seems, the relative focus for the agency's documentation correlates rather well with the relative focus of the controls in ISO/IEC appendix A, the agency seem partly to fulfil the security policy which it has defined itself, the metrics connected to ISO/IEC appendix A shows that most of the controls listed (76%) do not have an entity assigned to it (meaning there is no one appointed to be responsible for the action), and the agency tend to focus on operative matters and on acting when something has happened, rather than emphasize planning and developing and carrying out proactive information security work.

6. Discussion

Bearing in mind that this is still work in progress, we would like to underline a few issues.

We started at the communication processes which catch the communication structure in an organization in general. Communication is viewed as equal to steering and control; where in general messages about what to do are sent from one entity to another while controls are fed-back to check on the status of the processes. Since information systems contain both technical and non-technical parts, the flow of all messages and control loops need to be represented in a model of the communication. We introduce a model, called the 14 layer Framework, which allows exactly this: it includes the technical layers, relying on the ISO/IEC 7498-1 (International Standards Office, 1998), and the non-technical – called social – layers, relaying mainly on work by Kowalski (1994), FRISCO (Falkenberg et al., 1998) and Langefors (1968). The full analyses are presented in two COINS reports (Yngström et al., 2009a, Yngström et al., 2009b). The contribution, apart from marrying technical layers with social

layers are two adaptation layers; one for internal adaptation and one for external adaptation, which also is in line with system theories.

The framework needs a vocabulary/taxonomy in order to express statements of steering and control. This is constructed based on established lists of security related terms. Definitions of terms for the vocabulary rely on general dictionaries such as Concise Oxford English Dictionary (Oxford University Press, 2004) and 'http://en.wikipedia.org/wiki'. In addition concepts and definitions are compliant with Swedish standards (SIS, 2003). The full terminology is presented in Enclosures to COINS report #1 (Yngström et al., 2009b) and the applicable definitions are presented with examples in chapter 4 and 5 of COINS report #1 (Yngström et al., 2009a). The approach to use a general dictionary complemented with standard security definitions was chosen to emphasis the fact that security is not a special issue but an issue of control. This approach makes it possible to relate the general terminology to the 11 normative security controls, A5-A15, from the ISO-27001 (International Standards Office, 2006). Thus the reference model used for computation of distribution over A5-A15, including the comparisons between the ideal, the decided policy and the security praxis, can all be expressed using the constructed taxonomy. As for the feasibility of work, we rely partly on the feedback from the agency in relation to the practical findings, partly on discussions on how to proceed. Given that the results are in line with the agency's own picture, the proceeding work can be more streamlined and focused. For other researchers we can also offer our transcribed interviews.

7. Acknowledgments

This work was supported by the Swedish Civil Contingencies Agency

8. References

Ackoff, R. (1976), Designing a National Scientific and Technological Communication System, University of Pennsylvania Press, 1976.

Ashby, R. (1963), Introduction to Cybernetics, Wiley & Sons.

Avizienis, A., Laprie, J., and Randell, B. (2001), Fundamental Concepts of Dependability, Research Report No 1145, LAAS-CNRS.

Beer, S. (1964), Cybernetics and Management, Science Edition, John Wiley, New York.

Beer, S. (1979), The heart of the enterprise, John Wiley & Sons.

Beer, S. (1981), Brain of the Firm, John Wiley & Sons.

Boulding, K. (1964), "General Systems as a point of view", in Mesarovic, M. D. (Ed.) Views on General Systems Theory, John Wiley & Sons.

CC (2009), Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Information, Version 3.1, Revision 3.

Checkland, P.B. (1988), "Images of Systems and the Systems Image", Presidential address to ISGSR, June 1987, Journal of Applied Systems Analysis, Vol 15, pp 37-42.

de Rosnay, J. (1979), The Macroscope: A New World Scientific System, Harper & Row.

Falkenberg, E. D. et al. (1998), A Framework of Information System Concepts: The FRISCO Report, Leiden, The Netherlands: International Federation for Information Processing, IFIP.

Flood, R. (1999), Rethinking the fifth discipline: Learning within the unknowable, Routledge.

Hevner, A., March, S., Park, J., and Ram, S. (2004), "Design science in information systems research", MIS Quarterly, 28(1):75-105.

International Standards Office (2006), ISO/IEC 27001:2006, Information technology – Security techniques - Information security management systems – Requirements, Geneva: ISO.

International Standards Office (1998), ISO/IEC 7498-1, Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, Geneva: ISO.

Kowalski, S. (1994), IT Insecurity: A Multi-Disciplinary Inquiry, Doctoral Thesis SU/KTH Department of Computer and Systems Sciences. Report Series No. 94-004. ISSN 1101- 8526. ISRN SU-KTH/DSV/R–94/4–SE March 1994. ISBN 91-7153-207-2.

Langefors, B. (1968), Introduktion till informationsbehandling, Berlingska Boktryckeriet.

Miller, J. (1978), Living Systems, McGraw Hill.

Oxford University Press (2004), Concise Oxford English Dictionary, 11th ed. Oxford University Press Inc 1911. ISBN 0-19-860864-0.

Shostack, A. and Stewart, A. (2008), The New School of Information Security 1st ed., Addison-Wesley Professional.

SIS (2003), SIS HB 550: Terminologi för informationssäkerhet, utgåva 3, SIS Förlag.

Swedish National Audit Office (2007), Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen, RiR 2007:10.

Yngström, L. et al. (2009a), COINS report # 1 Modelling the Communication of Information Security Issues, DSV report series No 09-008A, Stockholms universitet, Sweden.

Yngström, L. et al. (2009b), COINS report # 1 Enclosures; Modelling the Communication of Information Security Issues, DSV report series No 09-008B, Stockholms universitet, Sweden.

van Gigch, J. (1978), Applied General Systems Theory, Harper & Row, New York.

von Bertalanffy, L. (1956), Main Currents in Modern Thoughts, in Yearbook of the Society for General Systems Research, Vol 1.

Wiener, N. (1948), Cybernetics or Control and Communication in the Animal and Machine, John Wiley & Sons.