

DISCOVERING INFORMATION SECURITY MANAGEMENT

Fredrik J. Björck

May 2005

We must plan for freedom, and not only for security, if for no other reason than that only freedom can make security secure. (Popper, 1945)

Publication Data:

Fredrik J. Björck

Discovering Information Security Management

Stockholm: Department of Computer and Systems Sciences

Stockholm University & Royal Institute of Technology

Report series No. 05-010, ISRN SU-KTH/DSV/R--05/10--SE

ISSN 1101-8526, ISBN 9171550755

Copyright © 2005 Fredrik J. Björck

Abstract

This thesis is concerned with issues relating to the management of information security in organisations, motivated by the need for cost-efficient information security. It is based on the assumption that: in order to achieve cost-efficient information security, the point of departure must be knowledge about the empirical reality in which the management of information security takes place. The data gathering instruments employed are questionnaires with open-ended questions and unstructured research interviews. The empirical material is analysed, and conclusions are drawn following the principles Grounded Theory. Data sources are professionals in the area of information security management, including information security consultants ($n=13$), certification auditors ($n=8$), and information security managers ($n=8$). The main contributions are; an integrated model illustrating the experts' perceptions concerning the objectives, actors, resources, threats, and countermeasures of information security management, a framework for the evaluation, formation, and implementation of information security management systems, a new approach for the evaluation of information security in organisations, a set of success factors concerning the formation of information security management systems, and a problem inventory concerning the value and assessment of information security education and training.

Acknowledgements

This doctoral process has taught me very much about research, myself, and the world. It took longer than I had originally planned. I came in as a boy and I leave as a man, and a father. There is nothing on earth I would like to exchange these years for. Thank you God. I have met so many people on my doctoral path, and I would like to thank You all.

Swedish Standards Institute, the Swedish Information Processing Society, the Swedish information security community, all the respondents and interviewees who formed the empirical foundation for this thesis. Without the link to You - the practitioners of information security, this would not have been possible. Thank you.

My advisor Professor Louise Yngström for always being there, for giving me deadlines, for deciding to employ me back in 1998, and for being a good friend and colleague. The SecLab family. The leadership and the administration of the department, for financing and administrative support throughout the years. Rick Downes, co-founder and consultant of Rixstep, for proof-reading the English, and for coaching. Dr. Kjell Näckros, Dr. Christer Magnusson, Dr. Eriks Sneiders, Dr. Danny Brash, and Dr. Janis Stirna, for being both friends and colleagues. Kjell for his support during the writing-up, Christer for sharing his knowledge on information security in organisations, Eriks for his entrepreneurial spirit, Danny for his insights on qualitative research methods, and Janis for all those exciting fishing trips, and for giving many detailed comments that improved this work. The entire DSV family.

Bo Johansson and Christer Karlsson, my friends, without Your support, this would not have been possible. Johan Blix, Alja Skirgård, Charlotte Björck and Sofie Björck - my parents and sisters, for always being there. Kajsa-Stina, for taking care of our daughters Lovisa and Filippa, and their grandmother Hilkka - without You, this would not have been possible. I often think about Professor Terttu Orsi, Anna Dufvenstierna, and Professor Bengt G. Lundberg - I know You are here with us. Thank You!

To Lovisa and Filippa.

Contents

I	Introduction and summary	13
1	Thesis overview	15
1.1	Thesis structure	15
1.2	Problem area and motivation	16
1.3	Research method	17
1.4	Contributions	18
1.5	Conclusions and implications	19
II	On Information Security Management Systems	21
2	Introduction	25
2.1	Background to the research	25
2.2	Research questions	28
2.3	Justification for the research	30
2.4	Summary of contributions	32
2.5	Quality and limitations of this work	34
2.6	Further work	37
2.7	Outline of this part of the thesis	37
3	Research strategy and research methods	39
3.1	The choice of a research strategy	39
3.2	Modified action research strategy	41
3.3	Limitations of action research	44
3.4	Data collection and analysis methods	45
4	ISMS framework	47
4.1	Framework introduction	47

4.2	Proposed ISMS process model	49
4.3	Evaluation stage	52
4.4	Formation stage	56
4.5	Implementation stage	59
5	Evaluation stage	63
5.1	The software tool	64
5.2	The evaluation approach	68
6	Formation stage	83
6.1	Introduction	84
6.2	Research method	86
6.3	Certification auditors' perspective on formation and cer- tification of ISMS	90
6.4	Information security consultants' perspective on forma- tion and certification of ISMS	96
6.5	Conclusions	101
7	Implementation stage	105
7.1	Introduction	106
7.2	The individual's perspective	108
7.3	The organisation's perspective	121
7.4	Conclusions	130
III	On the Management of Information Security	133
8	Introduction	137
8.1	Background to the research	137
8.2	Research problem and contributions	138
8.3	Justification for the research	139
8.4	Methodology	141
8.5	Outline of this part of the thesis	142
8.6	Definitions	142
8.7	Delimitations of scope and key assumptions	144
8.8	Chapter summary	146

9	Methodology	147
9.1	Overview of Grounded Theory	147
9.2	The principles of Grounded Theory	148
9.3	Research method of this study	149
9.4	Personal background and influence on the research process	152
10	Analysis of Data	155
10.1	Introduction	155
10.2	Analysis of objectives	156
10.3	Analysis of actors	159
10.4	Analysis of resources	163
10.5	Analysis of threats	166
10.6	Analysis of controls	171
10.7	Chapter summary	174
11	Conclusions and implications	175
11.1	Conclusions about the research problem	175
11.2	Implications for theory	177
11.3	Implications for practice	179
11.4	Further research	179
A	WCC Revisited	183
A.1	The Model	184
A.2	The Approach	188
A.3	The Result	189
A.4	The Discussion	193
A.5	The End	194
B	Revisorernas syn	195
B.1	Bakgrund	195
B.2	Metod, demografi och reliabilitet	196
B.3	Framgångsfaktorer för införande	198
B.4	Svårigheter och utmaningar vid certifiering av LIS	203
B.5	Fokus och tyngdpunkter i LIS-projekt	206
B.6	Övriga kommentarer	209
C	Konsulternas syn	211
C.1	Bakgrund	211
C.2	Metod, demografi och reliabilitet	212

C.3	Framgångsfaktorer för införande	214
C.4	Metoder och metodverktyg i 7799-projekt	222
C.5	Fokus och tyngdpunkter i LIS-projekt	224
C.6	Övriga kommentarer	227

D Contribution to SBA Check 231

E Thematic Interview Synopses 235

E.1	Interviewee 01	235
E.2	Interviewee 02	242
E.3	Interviewee 03	246
E.4	Interviewee 04	249
E.5	Interviewee 05	253
E.6	Interviewee 06	256
E.7	Interviewee 07	261
E.8	Interviewee 08	265

List of Figures

2.1	The optimum level of security – illustrating the balancing act of security management.	26
2.2	The Information Security Management Process (ISMS Process).	29
3.1	Factors affecting the choice of a research strategy	40
3.2	The difference between the adopted research strategy and familiar action research.	42
4.1	The Information Security Management Process (ISMS Process).	50
4.2	The evaluation stage	53
4.3	The formation stage	56
4.4	The implementation stage	59
5.1	SBA Check main evaluation interface.	64
5.2	SBA Check report example.	65
5.3	Historical development of SBA Check.	67
5.4	Overview of the evaluation process.	69
5.5	Overview of the initiation stage.	70
5.6	Example of expectations on the evaluation.	71
5.7	Typical contents of an evaluation plan and agreement. . .	74
5.8	Analysis stage.	75
6.1	Illustration of how the empirical materials from the consultants are conceptually generalised – from single quotes via codes to categories - to form the theoretical framework - the sucess factors.	89

6.2	Success Factors for the formation and certification of information security management systems, from the certification auditors' perspective.	95
6.3	Success Factors, expressed as project capabilities needed, for the formation and certification of information security management systems, from the information security consultants' perspective.	100
7.1	Some general characteristics of the students	117
7.2	Expected payment flows resulting from investment in the microphone-manufacturing machine	124
7.3	The present value (PV) of investing in this alternative . .	125
7.4	The net present value (NPV) of investing in this alternative	126
7.5	Expected payment flows resulting from investment in the information security education and training programme .	127
9.1	The main user interface in Atlas.ti.	150
9.2	The network editor in Atlas.ti.	152
10.1	Focused network view: Security Objectives	158
10.2	Focused network view: Business Objectives	160
10.3	Focused network view: Actors	161
10.4	Focused network view: Physical Resources	165
10.5	Focused network view: Intellectual Resources	167
10.6	Focused network view: Threats	169
10.7	Focused network view: Controls	173
11.1	An integrated view of the results	176
A.1	A classification model for information security research. .	184
A.2	Applying the classification model to the 125 papers from the SEC 2000 proceedings.	190
A.3	SEC 2000; proportions of research papers in each domain.	191
A.4	SEC 2000; proportions of research papers at different levels of abstraction.	191
A.5	SEC 2000; types of contribution.	191
A.6	SEC 2000; types of tests.	192
A.7	SEC 2000; proportion of papers that contain evaluation results.	192

A.8	Greatest obstacles to addressing security concerns	193
B.1	Framgångsfaktorer för lyckat införande och certifiering av ledningssystem för informationssäkerhet enligt SIS (SIS, 1999b), ur certifieringsrevisorernas perspektiv.	202
C.1	Framgångsfaktorer för lyckat införande och certifiering av ledningssystem för informationssäkerhet enligt SIS (1999b), ur informationssäkerhetskonsulternas perspektiv.	221
C.2	Metoder och metodverktyg	222
D.1	Early design study of SBA Check	232
D.2	Primitive prototype of SBA Check	233
D.3	Current version of SBA Check (4.x)	234

Part I

Introduction and summary

Chapter 1

Thesis overview

1.1 Thesis structure

This doctoral thesis is composed of three parts:

- Part 1, Thesis overview
- Part 2, On Information Security Management Systems
- Part 3, On the Management of Information Security

Part 1 introduces the reader to the problem under study and summarizes the results and contributions of the thesis. Part 2 is concerned with *management systems* for information security. Part 3 is concerned with the *management of information security in general*.

The content in Part 2 has earlier been presented as a thesis for the degree of licentiate of philosophy, awarded the author by the Department of Computer and Systems Sciences, Stockholm University / Royal Institute of Technology (Björck, 2001b).

Each of the parts 2 and 3 have separate introductory chapters which describe in detail the background, research objectives, methods, and results. Therefore, the aim of this overview is to summarize and integrate the information found in these parts.

1.2 Problem area and motivation

This thesis is concerned with issues relating to the management of information security in organisations, motivated by the need for cost-efficient information security.

It is based on the assumption that: in order to achieve cost-efficient information security, the point of departure must be knowledge about the empirical reality in which the management of information security takes place. Thus, this thesis is inductively oriented, in that it draws its conclusions based on studies of the practice of information security in organisations.

Furthermore, the studies presented in this research are motivated by the relative lack of systematic empirical studies (as discussed in section 8.3) in the area of information security management. The aim is that this study, together with past and future empirical studies in the same area, will contribute to filling this gap, and thereby lay the foundation for a coherent body of knowledge, firmly based on the issues facing practitioners in this applied field. This foundation is needed if the research area concerned with managing information security in organisations is going to be successful in offering theories, models, methods, and tools useful for understanding, influencing, controlling, and predicting issues relating to information security management.

Within the broad area described above, this thesis tackles two main research problems. They are:

What problems do organisations face and what processes do they go through as they are aiming to establish a balanced management system for information security?

This question is studied in part 2 of the thesis. The question calls for the examination of three more detailed problems, relating to the *evaluation, formation and implementation* of management systems for information security. These questions are: *How can an organization*

evaluate its current state of information security? (focus in chapter 5) *What are the success factors to consider while creating a management system for information security?* (chapter 6) and, *What problems are related to measuring implementation effectiveness of information security education efforts?* (chapter 7).

The second research problem is:

What perceptions do information security managers hold as regards the management of information security in organisations?

This problem is investigated in part 3 of the thesis, by means of in-depth research interviews with senior information security managers, followed by an analysis informed by Grounded Theory.

1.3 Research method

This work has an empirical focus in that it starts with observations and goes from there to abstractions and models. It can be characterised as an inductive, explorative, qualitative, and systematic approach.

The approach taken was informed by Grounded Theory, and guided by the principles set forth by one of its originators (Glaser and Strauss, 1967; Glaser, 1978, 1992, 1998).

The data gathering instruments employed are both questionnaires with open-ended questions (described further in chapter 3 and in section 6.2), and unstructured in-depth research interviews (chapter 9).

Data sources were professionals in the area of information security management, including consultants ($n=13$), certification auditors ($n=8$), and information security managers ($n=8$). These were selected on the basis of expertise rather than on statistical sampling. It follows that the purpose was *not* to draw conclusions about the larger population from which the respondents and interviewees were drawn. The character of the study is ideographic rather than nomothetic.

Data analysis was carried out using a Grounded Theory-oriented approach, with the help of a software tool for qualitative data analysis called Atlas.ti (Muhr, 2004). This software offered a number of advantages compared to a manual approach, one being that it preserves the transparency of the analysis process. Specifically, it makes it possible to follow the line of thought back from the model, via categories, down to the quotations on which the model is built.

1.4 Contributions

The contributions for the different parts of the thesis are described in section 2.4 (for part 2) and in chapter 11 (for part 3). In summary, they are:

- **Integrated model** illustrating the experts' perceptions concerning the objectives, actors, resources, threats, and countermeasures of information security management.
- **Theoretical framework** for the evaluation, formation, and implementation of information security management systems.
- **New approach** for the evaluation of information security in organisations.
- **Set of success factors** concerning the formation of information security management systems.
- **Problem inventory** concerning the value and assessment of information security education and training.

The common denominator for all these is that they aim to contribute to solving problems related to information security management in organisations.

1.5 Conclusions and implications

Owing to the nature of the research problem and the research design, the research questions cannot be answered in a single sentence, nor can all the conclusions be spelled out in this single concluding section. Instead, the answers to the posed research questions are found throughout the thesis. Conclusions and implications are explicated in sections 5.2.6, 6.5, and 7.4 for part 2, and in chapter 11 for part 3.

The main aim of this study has been to "map up" or "discover" the - to an extent unknown - terrain of information security management in organisations. By offering a framework for the evaluation, formation and implementation for information security management systems, and by identifying the basic building blocks of information security management (its objectives, actors, resources, threats and controls), this study contributes practically and theoretically.

Practitioners can use the results presented here as "blueprints" for managing information security. They can compare and benchmark their own processes and practices against these results and come up with new critical insights to aid them in their work.

Scholars in the field of information security management can use the results here, and build further on them, to form a coherent and complete body of knowledge of the area - all with the aim that we should be able to create models and theories that help practitioners understand, influence, control, and predict what goes on in their organisations.

Part II

On Information Security Management Systems

This part of the thesis presents the findings of an empirical study into the evaluation, formation and implementation of information security management systems aiming to protect organisational information assets. An action research oriented strategy and a research method informed mainly by grounded theory, are employed. The main results of this study are 1) a blueprint process for information security management, 2) an information security evaluation method, 3) success factors for creating balanced information security management systems, and 4) a discussion on problems related to measuring the effects of information security education in an organisational context.

Chapter 2

Introduction

2.1 Background to the research

Too much business security will increase your costs and reduce your potential revenue streams substantially (*ceteris paribus*) and it can – in due course – put an end to your business. To “run the risk” is in fact at the heart of entrepreneurship; American economist Knight pointed out that “profit, earned by the entrepreneur who makes decisions in an uncertain environment, is the reward for bearing uninsurable risk” (Knight, 1921). Conversely, insufficient security might leave your business open for fatal mistakes, espionage, sabotage and crime. The goal of security management in organisations should therefore be to identify and strive toward the optimal point between security and insecurity.

The optimum level of security in an organisation (Fig. 2.1), from a strict financial perspective, will be found in the situation where the cost of *additional* security countermeasures *exactly equals* the *resulting* reduction in damages arising from security breaches (Marin, 1992). This level of security means profit maximisation for the organisation. Too little security means that security breaches are reducing profits as a result of damages to assets, and too much security means that the costs

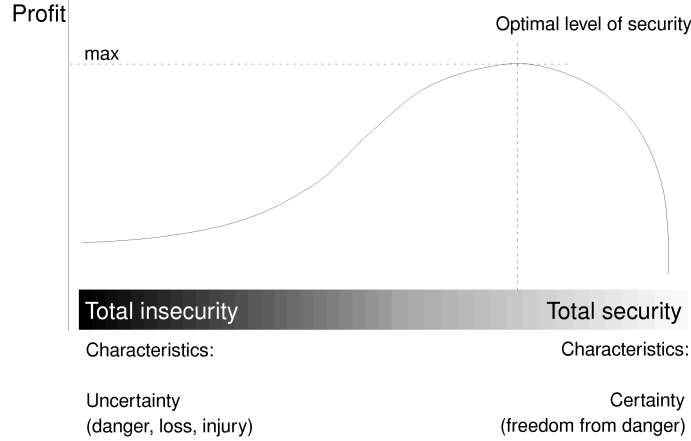


Figure 2.1: The optimum level of security – illustrating the balancing act of security management.

of security countermeasures (including operational ineffectiveness and high-end security solutions) consume profits (Björck, 1996). Hence, we should not strive towards higher and higher security without thinking about the consequences. Moreover, security measures have other consequences than strictly monetary to be taken into account, *e.g.* social, legal and ethical. Opposing views from various groups of stakeholders to the organisation will also have to be recognized.

In practice, it is problematical to identify the security equilibrium depicted here. There are solutions available, *e.g.* the one created by Longley and Kwok (1996) which can be employed to help security managers deploy security resources in an optimal way. However, in many cases, the total cost of current security countermeasures and the damages arising from current security breaches are not known. And, looking into the future, the potential costs-and-benefits of new countermeasures are even more challenging to estimate (Adams, 1995). To further complicate things, this research is not on protecting organisational assets

in general – it is about protecting *information assets*. It is difficult to assess the value of a given information asset, since it mainly depends on what it can be used for in the future (Falk and Olve, 1996; Glazer, 1993). Also, it is not always noticeable that an information asset has been subject to a security breach – if it *e.g.* has been changed by mistake or disclosed to an unauthorized party. As a result, it is problematic to devise economically optimised information security measures.

It is widely agreed that organisations in reality do not behave strictly according to a profit-maximising economic model (as that in Fig. 2.1). Instead, decisions and behaviour are characterised by, at best, bounded rationality and trying to satisfy objectives rather than reaching them (Simon, 1948; Cyert and March, 1963). Hence, it is important to keep in mind that the model used here is an *ideal model* from the point of view of the owners of the organisation, aiming to clarify the problems faced.

Despite the difficulties outlined above, organisations need to at least try to estimate: a) the current level of information security; b) the ideal level of information security; and c) how to get from *a* to *b*. Although this research will not conclusively *solve* any of these issues, it is concerned with all three.

Several recent studies demonstrate the need for organisations to systematically approach the protection of their information assets:

- Computer Economics estimates that for 2001 (as of the end of August) the economic impact of virus attacks around the world has hit \$10.7 billion (Computer Economics, 2001)
- 85% of the 528 U.S. organisations responding to the CSI/FBI survey detected computer security breaches within the last twelve months and 64% acknowledged financial losses due to those breaches (Computer Security Institute, 2001)
- 66% of the 273 European CIOs and business executives interviewed in the Ernst & Young Information Security Survey cite information

security or privacy concerns as a major inhibitor to greater use of e-commerce (Ernst & Young, 2001)

- In Sweden, 84% of the respondents ($n=428$) to the Information Security Survey had suffered economic losses due to breaches of information security, as compared to only 56% of the respondents ($n=541$) the year before (Björck, 1997, 1998).

Adding to this the rapidly increasing dependence of information and IT systems, the need to manage information security is apparent.

2.2 Research questions

The research tackles certain aspects in connection with the following question:

What problems do organisations face, and what processes do they go through, as they are aiming to establish a balanced management system for information security?

This question does not have *one* answer – it has *many*: Organisations have different goals, strategies, organisational cultures and structures; consequently the ideal management system and the way to achieve it will differ between organisations (Mintzberg, 1983). Acknowledging this – the need to cater for situational context – this part of the thesis proposes a framework instead of a comprehensive information security management methodology. Organisations and researchers can use the framework to “plug-in” preferred approaches, fitting to the context of the problem at hand. Beyond the framework, this part of the deals with sub-problems within the broad research question. It also attempts to build a tentative “plug-in” methodology for a part of the framework.

In correspondence with the research question above, the framework for the study – presented in detail in next chapter – is a process view of the activities included when an organisation seeks to arrive at a balanced

management system for information security. Henceforth, we shall refer to this as the information security management system (ISMS) process. A high level view is presented here to illuminate how the *specific research questions* contribute to the study at large. Each of the revised

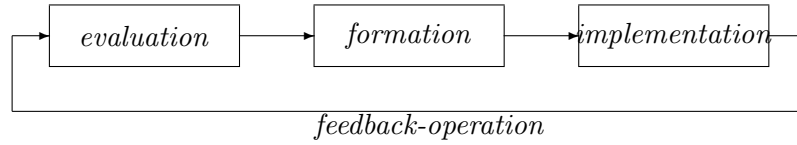


Figure 2.2: The Information Security Management Process (ISMS Process).

and extended papers presented in this parts' main body is positioned within one of the three main stages of the ISMS process – *evaluation*, *formation*, and *implementation* (please refer to the next chapter for a detailed description of these).

The research question related to the *evaluation stage* of the ISMS process is:

- 1) *How can an organisation evaluate its current state of information security?*

This question is answered by offering a tentative evaluation methodology and an associated software tool. The Swedish Information Processing Society and leading information security experts in Sweden, in close cooperation with this research project, designed and built the software tool. The evaluation methodology was developed as a part of this study. This work is presented in chapter 5.

The research question related to the *formation stage* of the ISMS process is:

- 2) *What are the success factors to consider while creating a management system for information security?*

The answer to this question is sought using questionnaires to certification auditors and information security consultants all working in projects aiming to create management systems for information security corresponding to the ISO/IEC 17799 standard (SIS, 2001). This work is presented in chapter 6.

The research question related to the *implementation stage* of the ISMS process is:

3) *What problems are related to measuring implementation effectiveness of information security education efforts?*

This question is mainly tackled analytically using simple ROI-models (return on investments) from financial economics to illustrate the problem of measuring implementation effectiveness with regards to the human side of the information security management system. This work, parts of which are co-authored with Yngström is presented in chapter 7.

The ISMS process, as described here and in detail in the following chapter, illustrates a range of problems and promising solutions to many activities involved in evaluating, forming and implementing a management system for information security in an organisation. The intention is not to present it as the main *result* of this study. The framework should be viewed as an *ideal model* meaning that *it does not claim* that “this is the way all organisations do”, or “this is the way all organisations have to do”. Rather, it serves as a *framework* for this thesis part pointing out critical problem areas that are investigated and indicating how these fit together. It is also important to note that this study does not solve all problems in the ISMS process – it merely confronts some of these.

2.3 Justification for the research

The current state of – and the ensuing need for – information security was demonstrated earlier (section 2.1) by referring to several recent stud-

ies. In addition, the development of information security management on the international and national (Sweden) arena further accentuates the need for this study:

ISO, International Organization for Standards, recently promoted the British standard on information security management (British Standards Institute, 1999, 1995) to an international standard, ISO/IEC 17799 (ISO, 2000). Many organisations are now striving to meet the requirements of the standard. To do this, they will have to demonstrate that they have a management system for information security that is adequately protecting their information assets. The standard does not mention, however, *how* this can be attained. That is exactly the focus of this study. In Sweden; since the beginning of 1998, the Swedish Standards Institute (SIS) has worked to create and market a Swedish version of the cited British standard (British Standards Institute, 1999, 1995). It succeeded in 1999, when Sweden as one of the first countries adopted it as Swedish Standard 62 77 99 (SIS, 1999a,b). As a part of this undertaking, SIS formed a *pilot certification group*, later reformed into an *experience group* aiming to better understand and interpret the requirements of the standard and – especially – *how* to achieve them. We have been documenting the experiences in these groups as a part of this study.

On the academic level, the aim of this undertaking is to contribute to the body of knowledge regarding information security management in organisations. This contribution will mainly be in the form of helping to increase the understanding of problems associated with the ISMS process. In addition, it is hoped that this study can fill a gap by presenting the issues from a Scandinavian perspective. In our view, different nations seem to interpret information security management in different ways, often directly corresponding to the existing corporate culture and management style.

During the course of this study, results have continuously been fed back to information security management practitioners and scholars

through different channels. The aim was to test the usefulness and relevance of the findings. The software tool presented in chapter 5 is now internationally available, through the Swedish Information Processing Society, to users – in both Swedish and English (Swedish Information Processing Society, 2001a). As of September 2001 it has over 200 licensed users, mainly Swedish organisations. Over 100 information security managers and consultants have attended courses in using the evaluation methodology associated with the software tool (in the latest course, 100% of those attending rated the course contents as “good” or “very good” in a course quality survey). The success factors presented in the *formation* chapter 6 have been fed back to information security practitioners in Sweden at various industry conferences and as a publication from the Swedish Standards Institute (see Swedish reports enclosed in appendices). Major parts of this study have been accepted and presented at international academic conferences on information security in Sweden, Australia, China, and the USA. In summary, we feel that the partial results fed back so far have proved valuable to both academia and practice. Therefore, it is our anticipation and aspiration that this work – now presented in its entirety – will prove useful and relevant to these two audiences.

2.4 Summary of contributions

2.4.1 Contributions related to information security management in general

By modelling the ISMS process – with the stages *evaluation*, *formation*, and *implementation* – we have provided a blueprint process against which organisations attempting to attain a management system for information security can benchmark their current practices. The proposed ISMS process may also serve as a didactic instrument in education and training for explaining the interdependent activities involved in infor-

mation security management. On a more general level, this study has showed that information security management is not only about technicalities and engineering, but also about the human side of enterprise – people. Hence, one contribution is that it has helped to shift the focus away from computer system security to information (systems) security.

2.4.2 Contributions related to the evaluation of information security and ISMSs in organisations

By offering a tentative evaluation methodology and associated software tool, we have already started to fill in the details of the ISMS process. By explicating the methodology and the ideas behind it, and by building in flexibility in the software tool, organisations that feel that the methodology does not suit their corporate culture or evaluation situation can adapt it to better suit their needs.

2.4.3 Contributions related to the formation (design, development) of information security management systems in organisations

This study has contributed through identifying a set of success factors associated with the formation of a management system for information security in organisations. Organisations facing this challenge will probably find this relevant and beneficial, since it enables them to avoid now recognized pitfalls and capitalize on known winning techniques. Moreover, the hunt for success factors showed that the core problems associated with creating an information security management system are akin to those problems confronted in any organisational change effort. This might be viewed as a contribution in itself, since it opens up a whole new avenue of theories, tools and methods for information security management.

2.4.4 Contributions related to the implementation of information security management systems in organisations

We contributed through identifying the problems associated with measuring effectiveness of education programmes as a part of the implementation of information security management programmes in organisations. Specifically, the main contribution of this part was to identify the need for measuring the effects of education and training in this context, and also pointing out some major obstacles *vis-à-vis* measuring. The papers also shows the consequences of many organisations' fixation to "monetize" and compare their investments, including those into knowledge.

2.5 Quality and limitations of this work

Lincoln and Guba (1985) proposed four concepts that taken together may be used to demonstrate the soundness of a qualitative research approach – credibility, transferability, dependability, and confirmability:

2.5.1 Credibility aspects

Credibility – do the findings presented accurately reflect the reality studied?

Social reality is not a fixed reality that we can go out and study. On the contrary – it is a constantly moving target – and it is constantly being constructed. For that reason, there is no *one* reality, and therefore not only *one* truth about it that we can hope to find. Instead, there are multiple realities and multiple views. The question of credibility then is the question of if this study is "credible to the constructors of the original multiple realities" (Lincoln and Guba, 1985, : 296). As will be demonstrated in the next chapter, results of this study have been fed back on a continuous basis to these "constructors" to ensure that what is written in this thesis gives a truthful account of the studied phenomena.

However, we acknowledge that the background and pre-understanding on the part of the researcher does *influence* the findings, and especially how these are presented.

2.5.2 Transferability aspects

Transferability – are these findings useful for others in similar situations?

A qualitative research design, like this, makes it problematic to generalize findings back to a stated population. On the other hand, it gives a much richer and deeper understanding and description of the studied phenomena. It is important to point out that this study cannot, and should not, be taken as a description of how “it is” in *all* organisations – that was not the intention. On the ideographic – nomothetic – dimension, this study does not search for general laws of information security management (nomothetic) – no, it looks to describe specific problems, processes, and events, so that we can better understand these (ideographic). Nevertheless, if this knowledge could not be of use for others, it would not be worth the effort. By stating the boundaries and contexts within which this study has been undertaken, the reader can judge whether this knowledge could be of any use in another situation. Given that this thesis is based on a Scandinavian perspective and organisational culture, it might prove more valuable to organisations with similar values and management styles.

2.5.3 Dependability aspects

Dependability – would the results be repeated if the study was replicated?

Dependability corresponds with what in natural sciences is called *replicability*, which is the extent to which an application of equivalent instruments to the same units yields similar results. Since qualitative stud-

ies by their nature cannot be replicated, because of changing realities, the attention is turned to the stability and consistency of the inquiry process. Dependability for this study can be determined by auditing provided descriptions of data collection and analysis, studying the data itself, and contrast this with the findings. So even though replicability seems impossible, there are still methods to judge the soundness of this study. Replicability is problematic in all studies, since everything in our world changes, and since it is difficult to ensure that the instruments (like a microscope) and processes used in the re-inquiry are sufficiently equivalent to those used in the original inquiry.

2.5.4 Confirmability aspects

Confirmability – do the data help confirm the findings?

As discussed above, objectivity on the part of the researcher seems problematic. Still, we need to be assured that the findings are not only the imagination of the researcher. Using a qualitative research design, we do not depend on the researcher's objectivity – instead we turn our attention to the data or empirical materials. Were possible, we have tried to include the data directly in the thesis, such as the numerous quotations in chapter 6. In other parts, data is available on request, such as in the case of appendix A. There are parts, however, where it is difficult to provide data, since they build on an extensive period of participant observation. Although there are notes and documents from meetings, they do not give the full picture of the empirical materials gathered. In these cases, such as in chapter 5, it is still possible to confirm the soundness of the findings by going back and asking other persons that have been partaking in the same group or project. Even though we have done our utmost to ensure that everything written in this thesis is in line with the interpretations of the informants, it should be pointed out that the text in this thesis is also an interpretation – of that first interpretation.

2.6 Further work

Evaluation and refinement of SBA Check. As it stands, SBA Check and the evaluation approach presented in chapter 5 is not formally evaluated. The first step in this direction would be a survey to all licensed users of the software, focusing on the use of the tool, the perceived efficiency, the results, *etc.* A study like this, in cooperation with the Swedish Information Processing Society, is in its design phase.

Interview with experts. Another idea that has grown stronger during this study is to interview acknowledged experts on the management of information security in organisations, and to analyse these interviews in line with the ideas of grounded theory to search for themes and patterns in their views on the issue at hand (this is the focus in part 3 of the thesis).

Case study in organisation. Most of the material presented in this thesis is *general* in the sense that it does not *directly* tackle the sometimes chaotic reality in which organisations have to try to solve their information security problems (this study, as explained in section 3.2, has been on another level). In the practical situation, where abstract methods and loosely described security measures have to be interpreted and transformed into reality, other problems often emerge. Therefore, it would be very valuable to study various organisations in their efforts to manage information securely.

2.7 Outline of this part of the thesis

The next chapter (3) outlines the research strategy and chapter 4 describes the framework used to unify the different parts of the study, and form the base of the remainder of this thesis part. Readers mainly interested in practical utilisation and application of the findings can pass over chapter 3 and go directly to chapter 4 where the information security management systems process model is described. Chapters 5, 6,

7, each presents aspects of *evaluation*, *formation*, and *implementation* (respectively) – this is where the main studies of this part of the thesis are presented.

Chapter 3

Research strategy and research methods

3.1 The choice of a research strategy

The management of information security in organisations has been fruitfully studied using a variety of research strategies, such as action research, case studies, and surveys¹. The best possible research strategy to adopt is affected by number of factors, including: fundamental epistemological and ontological assumptions, the research context, the unit of analysis, and - logically - the research's problem and objective (figure 3.1).

Following is an explanation of how these factors have affected our choice to adopt an adapted version of *action research* as our basic strategy in this part of the thesis.

Type of research problem and objective. Barring the chapter concerning the implementation stage, the different parts of this part of the thesis describe research endeavours and results that are mainly of an *inductive* nature. The point of departure is the problems that

¹Refer to appendix A for a demonstration and discussion of different approaches and research foci in information security.

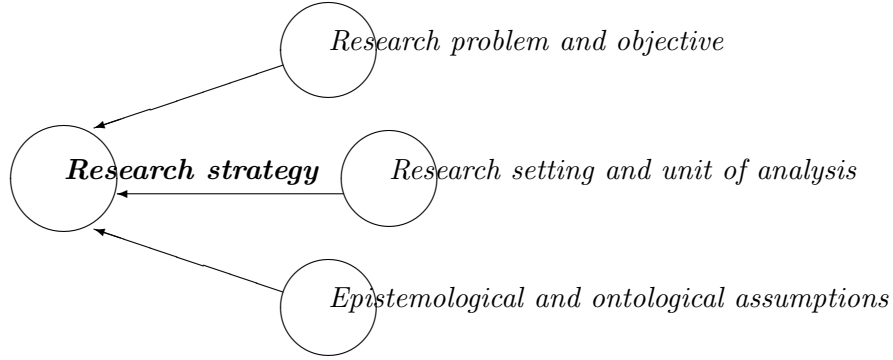


Figure 3.1: Factors affecting the choice of a research strategy

organisations face, and the processes they go through, as they are aiming to establish a balanced information security management system. The approach is essentially *explorative* and *descriptive*, aiming to discern and understand these problems and processes.

Research setting and unit of analysis. Empirical materials (data) are elicited from project groups formed with the purpose of discussing, understanding, and suggesting answers to these problems for practitioners. The findings presented in this part of the thesis are based on our participation in these groups over the course of circa two years. The nature of our partaking - i.e. to participate as researchers - was explicated and agreed upon at the outset. The participation has - with intent - been one of active involvement, not only as observers, but also as active group members.

Fundamental epistemological and ontological assumptions. This research is built on an underlying *interpretive epistemology*, in that we assume that the management of information security in organisations ideally should be explored from the frame of reference of those who are directly involved in these processes. Hence, this research could be classified within what Burrell and Morgan (1979) would call the interpretive paradigm:

The interpretive paradigm is informed by a concern to understand the world as it is, to understand the fundamental nature of the social world at the level of subjective experience. It seeks explanation within the realm of individual consciousness and subjectivity, within the frame of reference of the participant as opposed to the observer of action. Burrell and Morgan (1979, 28)

Our ontological stance is that the social world, which forms substantial parts of an organisation, does *not* exist independently of the observer. Managing information security in organisations is mainly about trying to control certain aspects of the social world, through influencing human behaviour *a propos* information security. Likewise, a decision to change the security of a computer based information system has to be interpreted and carried out by a human, and it is therefore dependent on circumstances in the social world.

3.2 Modified action research strategy

The matters described in the preceding section shape the chosen research strategy. Initially, we did not label the strategy. Only after the studies were carried out was it found that the strategy employed in some respects resembled what in the methodology literature is referred to as an *action research* strategy. Nevertheless, there are significant differences between the adopted strategy and action research. “Action research aims to contribute both to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration within a mutually acceptable ethical framework” (Rapoport, 1970, 499). An action research strategy is essentially defined by four characteristics; it deals with a (i) practical research problem in a (ii) participatory style. In addition, the pursuit of (iii) change, though a (iv) cyclical research and feedback process, is considered an integral part

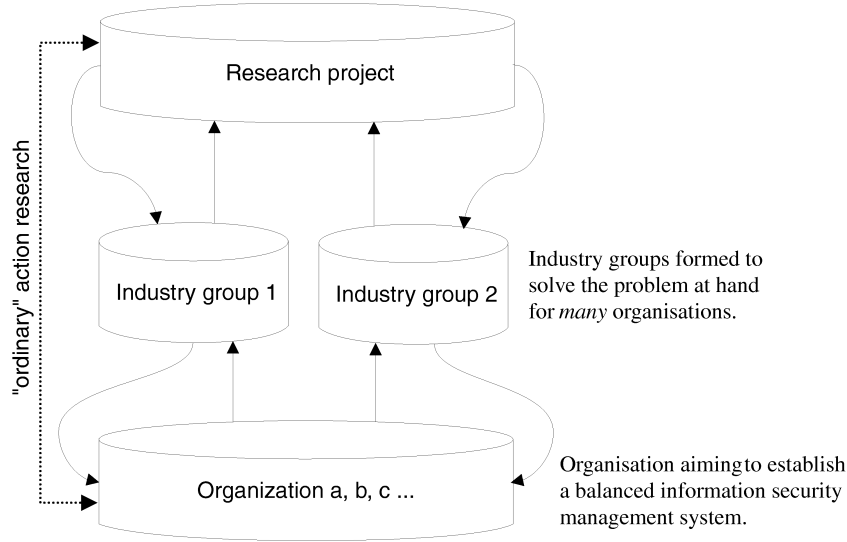


Figure 3.2: The difference between the adopted research strategy and familiar action research.

of research (Denscombe, 1998, 57). The following paragraphs briefly examine these defining characteristics in relation to this study:

Practical research problem. In this case, the research is concerned with the problems that organisations face, and the processes they go through, as they are aiming to establish a balanced information security management system. In Sweden, over 40 organisations have formed a group under the Swedish Standards Institute, named Project Information Security Management Systems *TK099*, aiming to work with these issues. As briefly mentioned above, a part of this research was carried out in that context (chapter 6). Another part of this research was done in cooperation with information security experts and the Swedish Information Processing Society (chapter 5) – also this of a direct practical nature. Therefore, the problems under study in this part of the thesis are clearly of a practical character. However, in action research litera-

ture it is often assumed that the problem solving and research process takes place *at the level of one organisation*, and that it deals with a problem in that very organisation. This is not the case here, as illustrated in figure 3.2. This means that the cycles of information gathering and feedback to/from the key sources - the organisations facing the problems studied - of empirical materials have been *indirect*. Thus, this approach is slightly different from that used in “ordinary” action research. This has undoubtedly affected the research results since some degree of analytical generalisation has already been done by the participants in these two industry groups (figure 3.2). As researchers in these groups, we – and our sources - have been comfortably positioned with some distance from organisations actually facing the problems. That has opened up the possibility to view the world as less chaotic and more structured – leaving us with a more idealised view of reality for better and for worse.

Participative. The pilot certification work group is unique in that it brings together certification auditors, information security consultants, government agencies, organisations interested in information security certification and researchers (us). All of these parties have been working together with the aim to generate and share the knowledge created. The respondents – the practitioners – have shared their own experiences and insights; we have merely summarized them in this study. They needed the knowledge themselves, which is why they decided to participate in the pilot certification group. We have participated in the pilot certification work group during the course of two years. Likewise, the Swedish Information Processing Society and the information security experts, together with whom we developed the evaluation tool and method presented later in this part of the thesis, were also participating to learn themselves and to help other organisations in their evaluation efforts.

Change. The third defining characteristic of action research is change, and reflection on the effects of change. Also here, the change instilled is indirect – on the level of the industry groups, so there is

very little reflection of the type “did this change do any good in the organisation?”, and more of a change and calibration of *views and ideas*. For example, the pilot certification group wanted to reach a common understanding of what is required for the successful implementation and certification of information security management systems according to the 7799 standard – they were seeking a methodology of how this could be done. The parties wanted to change - or calibrate - their views on these issues so as to reach consensus.

Cyclical feedback. The results were (and still are) fed back by means of presentations of what we have learned, and through written feedback reports. There are three target groups for this feedback: the practitioners in the projects (and in the study); the other information security and certification practitioners in Sweden; and the information security community at large – research as well as practice. This thesis is also a part in this cyclical feedback loop.

3.3 Limitations of action research

There are no research strategies without disadvantages – this is also true for action research. The main scientific objection to this kind of research strategy is that it can affect the “representativeness of the findings and the extent to which generalizations can be made on the basis of the results” (Denscombe, 1998, : 65), which is also noted by Baskerville (1999). This is true also for this study, but the objection assumes that the action research project takes place in only one organisation (a “work-site approach”). In contrast, this study is concerned with experiences and insights from *many organisations* and *many different contexts*, which may make the results more universal. Another objection to action research is that the researcher most likely cannot be totally detached and objective in relation to the subjects under study, since s/he is so immersed. This is against the positivistic ideas of research, as pointed out by for example Susman and Evered (1978). However, this fact can also

be viewed as a scientific advantage since it gives the researcher a closer and deeper view of what is studied.

3.4 Data collection and analysis methods

The specific research method used - within the defined action research strategy - differs from paper to paper (chapter to chapter) depending on the most suitable method for the problem at hand. Where relevant, each chapter describes the research process, principles and methods of the specific study. Among the data collection methods used are questionnaires, direct observation, participation, and documentary review. Methods for analysis of data applied are different types of qualitative analysis, such as the Grounded Theory-based analysis method offered by the software tool Atlas.ti (Muhr, 2004).

Chapter 4

ISMS framework

4.1 Framework introduction

Any organisation that wants to work systematically with information security will need to go through certain stages in pursuit of the goal of optimised information security. In essence, these resemble the common analytical stages we know from almost any type of ideal organisational - or even software development process:

- It is common to start out with some kind of analysis of where we are today and what we need to do to get where we want to be tomorrow.
- The next step is often to start describing or designing the ideas or solutions that will take us from the current situation to the identified ideal situation.
- Once these ideas or solutions are formed and explicated, they should be put into use in the organisation by some kind of implementation procedure.

As soon as the new ideas are used in the organisation, it is possible to gather information of how it works, with the aim of identifying further

room for improvement – a new change cycle can be initiated. There are many models available – especially within the quality management area – that describe these or comparable stages. For example the PDCA cycle, originally developed by statistician Shewhart and described in the quality management literature by Deming (1986). The PDCA cycle consists of the four stages: plan, do, check and act (Deming, 1986):

- *Plan*: Analyse the current situation to identify room for improvement and promising solutions.
- *Do*: Test the solutions on a small scale first in order not to disrupt critical processes.
- *Check*: Find out if the solutions are giving the expected results, and if they do:
- *Act*: Implement the solutions on a wider scale.

Models like these let us express the major activities involved from start to finish, or in this case from ‘problem faced’ to ‘problem solved’. The PDCA cycle is often used to describe organisational change processes. Lately it has often been used – at industry conferences and even in standardisation documents such as 7799 part 2 under revision (Humphreys, 2001) – to portray the activities involved in information security management projects. However, since the PDCA model was developed mainly to cater to the need of a systematic methodology when optimising automated manufacturing processes in the 1950s, it is not very well suited to describe the major activities in the ISMS process. For example, the *plan* stage includes both *analyses* of the current situation as well as *designing solutions*. In information security management, these two are most often rightly seen as two discrete activities. In addition, the *do*, *check*, and *act* stages clearly presume – although not explicitly - that it is possible to implement one small change and then measure its effect. This approach will work well for single, continuous improvements in an organisation (in

line with the Japanese total quality management philosophy, *Kaizen*¹). When implementing a new information security management system, however, we are normally attempting to bring more than a few significant changes to the organisation at once. In these cases, we have to wait with the *check* activities until the management system is already brought into play – when we can record feedback information from the ISMS in operation. For this, we need our own PDCA model that is tailor-made for information security management.

The next few sections will describe such a model, including its activities, the associated inputs and outputs, and major issues pertaining to each activity. The model will form the high-level framework for this part of the thesis.

4.2 Proposed ISMS process model

4.2.1 The need for a process model

The international standard for information security management - sometimes called the "ISO9000 for Information Security" - is primarily requirements oriented, meaning that it states the requirements organisations should satisfy if they want to undergo certification in accordance with the standard (ISO, 2000). It requires that the organisation has balanced its information security management system to counter the threats its information assets face. What is not spelled out in the standard though, is *how these requirements can be reached*. Many organisations here in Sweden, and in other countries as well, have been stalled in their plans to adhere to the requirements of the standard, since they simply did not know what steps to take to satisfy those. This was evident for most organisations in the Swedish pilot certification scheme. Although many organisations are hesitating to actual certification, many aspire to

¹The essence of the Japanese quality management philosophy *Kaizen* is to improve an organisation or a process continuously in small incremental steps.

adhere to the standard anyway, as it is seen to represent best practice in information security management. By proposing an ISMS process, and describing the activities involved, we take a first step toward resolving the problem depicted above. As always with process models, they can never be applied fully to any real world situation without first adapting them to the context at hand.

4.2.2 The ISMS process model evolution

This ISMS process model has been developed gradually through participation, observation, and interaction with information security consultants and other individuals working in projects trying to satisfy the requirements of the standard. At times, we have been immersed in one of the stages, and at other times, we have been concerned with the totality of the ISMS process and what it looks like. All organisations have their own methods and views. However, working together with some thirty individuals trying to interpret the standard, after more than two years of discussions and agreements and disagreements, we believe that the ISMS process model presented here is one that many practitioners and academics will subscribe to. The ISMS process model describes the stages and the important activities involved on a level of detail which still leaves room for situational adaptation.

4.2.3 High level view of the ISMS process model

The model divides the ISMS process into its sub-processes (figure 4.1).

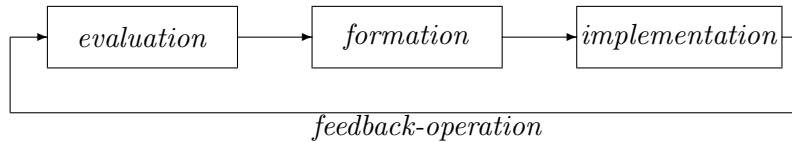


Figure 4.1: The Information Security Management Process (ISMS Process).

The *evaluation stage* includes everything it takes to assess the current situation vis-à-vis information security management in the organisation. It takes into account not only the administrative / organisational security issues, but also the technical (IT) security issues. The main results (output) of the evaluation stage are reports of vulnerabilities and deficiencies in relation to information security.

The *formation stage* takes these reports as its main input. It also adds knowledge about the organisation, its business processes, culture, etc. The goal is to design and develop solutions tailor-made to the organisation that will remedy any vulnerabilities and deficiencies in the current situation. The formation stage is largely analytical in that these solutions are still “on the drawing board”.

The *implementation stage* takes the solutions from the conceptual level and makes them work in the organisation. It entails for example installing and configuring technical security mechanisms as well as information security education and training to employees.

Once implemented, the ISMS is in *operation* and it starts to generate feedback information to the next iteration – as input into the new evaluation phase. Now, let us examine each of the stages more closely.

4.3 Evaluation stage

This section aims to discuss and clarify issues pertaining to the evaluation stage of the ISMS process. By doing this, it also lays a foundation for the coming chapters by providing explicit answers to questions such as: What is the subject of evaluation? What types of activities are generally associated with an evaluation? What does an evaluation result in?

4.3.1 Unit of evaluation

Information security evaluation methods (or, in some cases, frameworks) can take on many different forms and focus on a range of different aspects: The IT Baseline Protection Manual (Bundesamt für Sicherheit in der Informationstechnik, 2001), Orion (Fillery-James, 1999) and Odessa (Warren et al., 1997) can help evaluating the security of information or IT in an organisation. So can CRAMM (Insight Consulting, 2001) and SBA Scenario (Swedish Information Processing Society, 2001b), but from a strict risk/threat perspective. The SSE-CMM (SSE-CMM Project, 1999) can help evaluating a developers' systems security engineering capability, and the CEM/CC (NIST, 1997) the security functionality in (e.g.) an application system. If conducting an evaluation using CobIT (ISACF, 1996, 2000), the focus will be on management control over all activities in the IT department – some only indirectly related to information security. Evidently, there are many different security evaluation methods, and all of them have slightly different foci. This thesis has a special kind of evaluation focus in mind in the evaluation stage of the ISMS process. The unit of evaluation under study here is an ISMS and how it works in reality. An ISMS (information security management system) is the organisational infrastructure (it is not a computerized system) that enables information to be shared, whilst ensuring the protection of information and information processing assets (Brewer, 2000). It consists of a set of controls such as “policies,

practices, procedures, organisational structures and software functions” (SIS, 1999a, 7). Although the management system is declared in written documents such as the information security policy, it is not enough to identify and evaluate what is written in these documents. Instead, these written rules describe technical and administrative controls that exist in reality that can – and should – be evaluated.

4.3.2 An overview of the evaluation stage

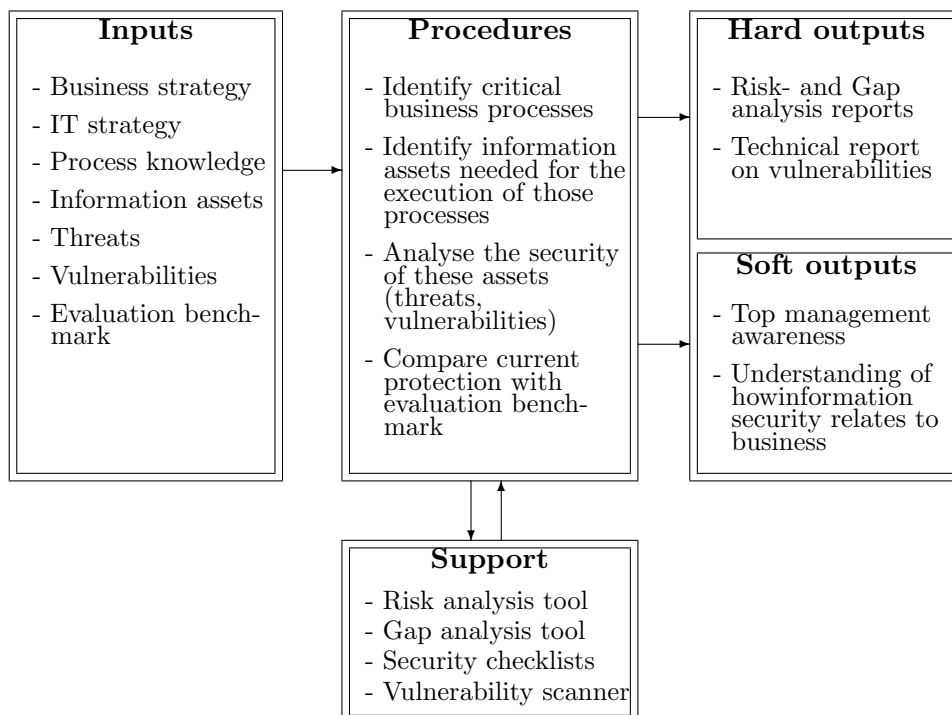


Figure 4.2: The evaluation stage

The goal of the evaluation stage is to assess the current information security situation of the organisation (figure 4.2). This evaluation takes into account not only the administrative / organisational security issues,

but also the technical (IT) security issues. Before any fruitful evaluation can take place, we need to gather some information:

Business & IT strategies. All organisations have a strategy, and many have it formally documented. In either case, here we can expect to find information about where the organisation is today (*e.g.* SWOT-analyses) and what it is trying to achieve (*e.g.* business objectives such as market share and profit), and how to get there (*i.e.* the strategy itself). In the evaluation stage we need to analyse both types of strategies (IT and business), so that we can elicit what business processes are critical in relation to the organisations' current strategy and objectives.

Process knowledge. Once the critical processes are identified, we need – as input – information about how these processes work in reality. Again, some organisations will have this formally documented with flowcharts of critical processes and associated activities. Other organisations might not have this documented, so sometimes this has to be done as a part of the evaluation stage. It is important to involve people with good knowledge of the process to be documented.

Information assets. We need to have a grasp of the organisations' information assets (*e.g.* information, databases, application systems, documents, *etc.*). There is no need to list all information assets in the organisation – this would be hundreds of thousands even in small organisations. It is only the information assets that are crucial to the successful execution of the identified critical business processes that should be included in the analysis.

Threats and vulnerabilities. Threats – such as fire, flood, and hackers – against the information assets should be considered. This can be done using a scenario technique (“What would happen if...”). Known technical vulnerabilities should also be used as input to

the evaluation stage.

Evaluation benchmark. We need some reference to evaluate against. When we know where we are today, we also need to be able to compare this to some ideal situation (where we want to be). This evaluation benchmark can be either the current information security rules of the organisation or a collection of best practices for similar organisations.

While describing the inputs, we have also started to express the procedures of the evaluation stage. First, we need to identify critical business processes and identify crucial information assets needed for the execution of those. Then we need to consider the consequences for the organisation if a threat against a certain asset would materialise. In addition, we need to look at the current protection for each asset and compare this with current rules or best practices. To aid in this work we can use a number of support tools such as automated risk- / gap analysis software, security checklists, and (IT) network- / system security scanners. These support tools can help in documenting and reporting findings, as well as automatically search large computer networks for vulnerable IT systems (all tools have serious limitations though).

The result of the evaluation stage is some kind of evaluation documentation, *e.g.* a report showing the result of the risk- / gap analysis efforts and documents showing vulnerabilities found in the current IT infrastructure. In addition to these “hard” tangible outputs, there are some important intangible or “soft” ones: By communicating the evaluation result to top management, their awareness for information security issues is heightened, and in many cases their support for the information security efforts in the organisation grows stronger. Also, the persons participating in the evaluation get an understanding of how information security related to business, as the connection from business objectives and strategy down to protection of information assets is illuminated.

4.4 Formation stage

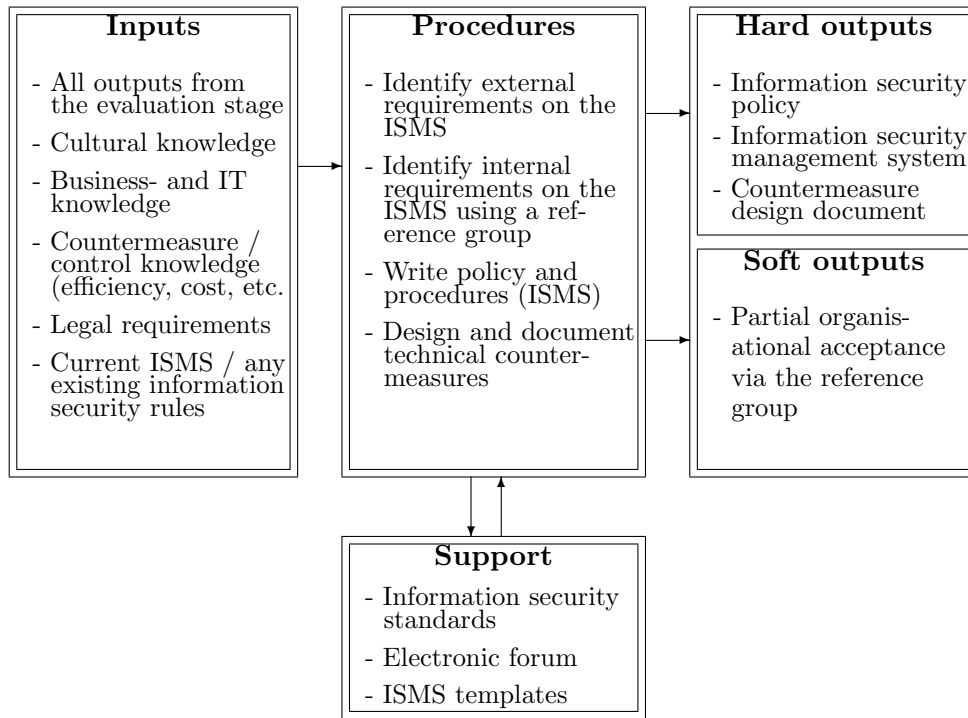


Figure 4.3: The formation stage

The goal of the formation stage is to design a technical and organisational infrastructure for information security that suits the business (figure 4.3). Such an infrastructure is documented as an information security management system – often presented in the form of a security handbook for the organisation. The written documents contain policies, rules and procedures with regards to how employees should handle information securely. In addition to rules aimed at humans, there is a need to create rules for many IT systems, *e.g.* “Only allow access from computer X” or “Require that all users change passwords within a 42 day cycle”. In the formation stage, we only design the solutions – they

are still only on the drawing board and not in the reality (that is for the next stage).

When forming the ISMS, we need information from different sources, so that we can create an ISMS that is suitable for the organisation:

Risk- / Gap-analysis reports, Technical security reports. These documents give us a view of the current state of information security, so that we know what we already have and where we start from.

Cultural, business and IT knowledge. The existing corporate culture can either enhance or hinder our efforts. Therefore we must have an idea of what it is like, *e.g.* what kind of behaviour is generally viewed as “ok” in the organisation. We also need knowledge of restrictions and requirements from the business and the current IT infrastructure. *E.g.* some parts of the organisation might require tighter security than others, and the current IT infrastructure might set limitations on what we can do in terms of network security.

Countermeasure / control knowledge. We need to know: what is available, to what cost, and what will it do for us? Countermeasures range from technical controls such as firewalls and access control and intrusion detection systems to information classification rules.

Legal requirements. Most countries have a data protection act, a legal framework for corporate governance (for financial accounting, etc.), and so on. Relevant laws have to be identified and the requirements on the ISMS from each law have to be taken into account.

Current ISMS / existing information security rules. If the organisation already have rules about information and IT security, these

have to be taken into consideration too, as they are the formal point of departure for the new ISMS.

Some of this information will be found in secondary sources like reports and existing policies, but most information will have to be brought into the formation stage through the involvement of people with that knowledge. Once we have the information at hand, we can list all the external and internal requirements on the ISMS, and then start to write the documents and design the technical controls deemed cost effective or required for other reasons. While doing this, it is helpful to have help from information security standards and templates, as they often include ideas of common countermeasures. If the project involves many persons or if the geographic distribution of the persons involved is wide, then it might be a good idea to do some of the discussions via an electronic forum especially set up for the project.

The result of the formation stage is a security handbook consisting of the information security policy and all rules and procedures, as well as a documentation of the chosen technical controls. The formation stage should be carried out using a reference group of persons from different parts of the organisation, because their knowledge is needed, and also because that is a part of the process of gaining acceptance for the ISMS in different parts of the organisation.

4.5 Implementation stage

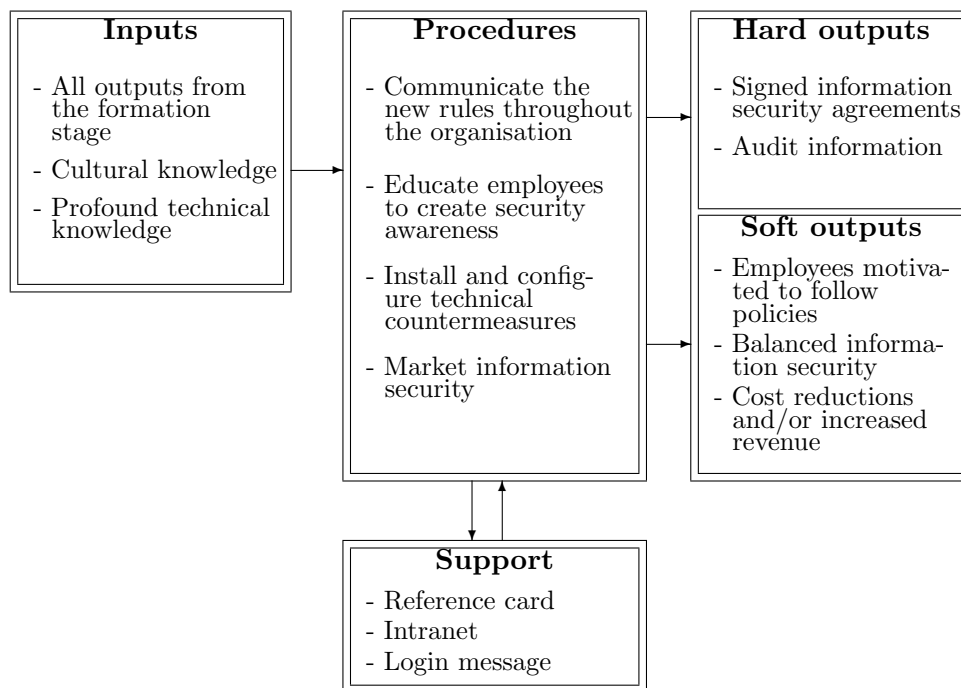
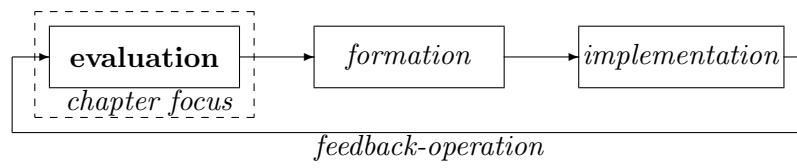


Figure 4.4: The implementation stage

The goal of the implementation stage is to take the ISMS, including also the technical controls, from the drawing board to reality (figure 4.4). This is the most difficult of all the stages, and it is also here that it will be evident if the other stages – the evaluation and formation stages – were carried out properly. The rules in the ISMS have to be communicated to relevant groups throughout the organisation, employees have to be motivated and educated and trained in using new technical security controls and following the rules agreed to in the ISMS. Also, all the IT-related solutions have to be installed or (re-)configured. Information security has to be marketed so that the organisation accepts adherence

to the rules laid out in the ISMS. This work can be aided by using a reference card or a brochure communicating the most important rules and explaining the most common technical controls (*e.g.* “This is how you use the anti-virus application”). If all goes well, the employees will sign off on and feel motivated to follow the rules in the ISMS. In that case, the result is that the organisation will have reduced the cost from security breaches and in some cases even enabled new streams of revenue in the future.



Chapter 5

Evaluation stage – Paper A: “Infosecurity Assessment Using SBA Check”

This chapter describes an approach for evaluating information security in organisations. The presentation is divided into one section on the software tool, and another on the method that can be employed when using the tool in conducting an evaluation¹. It should be noted that the type of evaluation proposed here is not the only kind of evaluation that needs to be done to get the full view of the information security situation in organisations. An example is the need for deeper analysis and evaluation of the security of critical IT systems that would not be completely covered by this approach.

¹This chapter is based on a previously published research paper (Björck, 2000). The original title of the paper was “Auditing Information Security Management Systems - Towards a Practical Method”

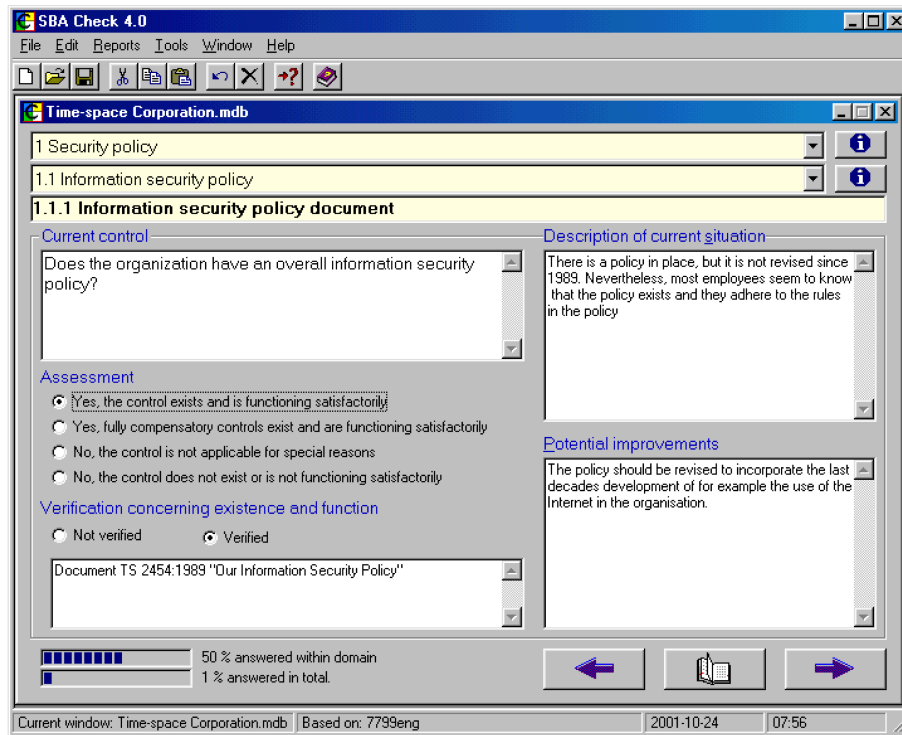


Figure 5.1: SBA Check main evaluation interface.

5.1 The software tool

5.1.1 Introducing SBA Check

SBA Check is a software application package which is aimed at supporting the evaluation of information security in organisations. As the name of the software tool indicates, it is a checklist-based approach to evaluation. This means that the evaluator(s) are guided through the whole evaluation process by means of searching for information and answering questions asked by the software tool with regards to the information security measures (controls) in the organisation (figure 5.1).

In addition to guiding the evaluator through an evaluation, the tool

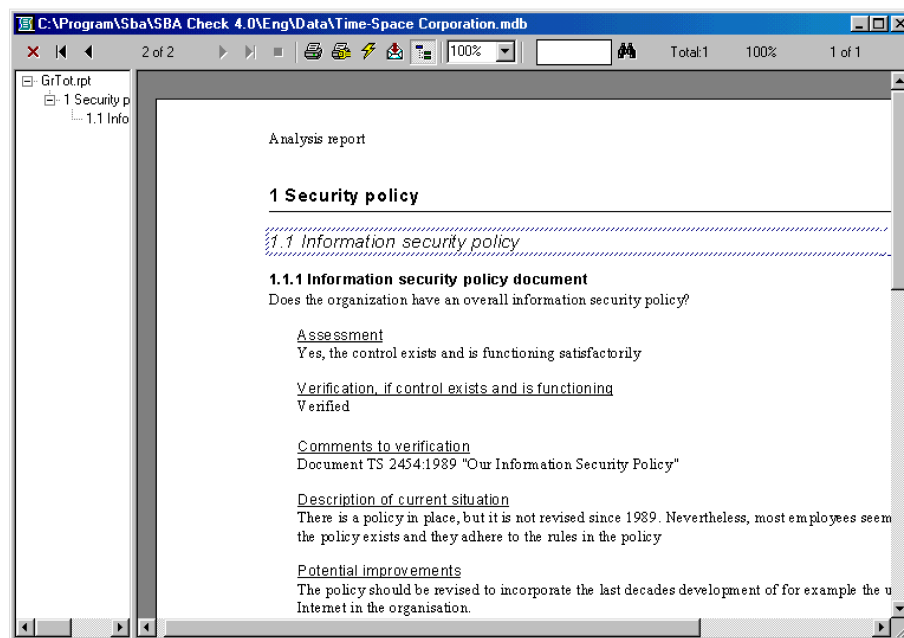


Figure 5.2: SBA Check report example.

helps to document the information security situation in a systematic fashion. For example, information regarding the current situation, potential improvements, assessment, any identified deficiencies for each security control present in the used checklist can be documented. Evaluators can learn how other organisations have solved similar security problems by turning their attention to the "best practices" database in the tool. One of the main ideas with this kind of tool is to enable the automatic generation of relevant reports to different stakeholders (figure 5.2). For example, graphical reports including descriptive statistics for top management and detailed reports for IT professionals responsible for developing and implementing solutions to resolve identified vulnerabilities and deficiencies are available.

5.1.2 Historic development of SBA Check

The Swedish Information Processing Society (SIPS) first released a tool called SBA Check in 1994². This was never widely used since it was not perceived to be very user friendly, even though it was excellent in theory. This version – 1 – focused on *IT systems security*, so it was a totally different tool than the current version. In 1999, SIPS had plans to revise the tool, and this is where we joined the development of SBA Check (figure 5.3). The result of the revision process was a totally different tool now focusing on information security in organisations. The first version – called version 3 – came out on January 20, 2000. The current version, as of December 2001, of SBA Check is 4.1. In terms of basic functionality, it is almost identical to version 3, even though some features have been added. One of the main improvements is that the tool is now available in English.

²Please note that SBA Check is one tool in a set of tools and methods marketed by the Swedish Information Processing Society, the latter often referred to as the 'SBA Method'. 'SBA' stands for 'SårBarhetsAnalys', the Swedish term for vulnerability analysis, and was originated in the early 1980s. Another related and well-known tool and method in the same family is that for risk analysis called 'SBA Scenario'.

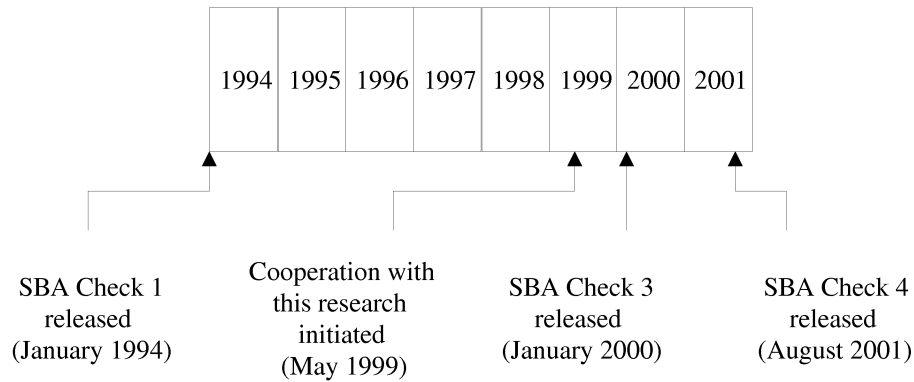


Figure 5.3: Historical development of SBA Check.

5.1.3 This research's contribution to the development of SBA Check

As the owner of the SBA Methods, the Swedish Information Processing Society initiated, financed and supervised the revision of SBA Check. Many organisations and individuals were involved in the process – from initial ideas, via requirements specifications and programming, to testing and later marketing. As the only academic representative in this group of information security experts and system developers, we assumed a key role in the development of SBA Check. Our specific contribution was the:

- Formulation of the working evaluation principles on which the tool is currently based and presenting these by means of a first version of the main user interface, and a primitive working prototype (see appendix D for details)
- Crafting of the requirement specification for the content of the tool, to be followed by content deliverers and the programmers.
- Development and documentation of a methodology for the evaluation process. This methodology is made explicit later in this

chapter.

SBA Check was created as a true team effort, and there were many other activities in the development of the software tool that are not listed here.

5.2 The evaluation approach

5.2.1 Introduction to the evaluation approach

The evaluation approach presented here can be employed, together with the methodology software tool *SBA Check*, for information security management assessment in organisations. The focus in this type of evaluation is on parts of the organisational management system for information security, such as information security related policies and procedures. Critical technical security mechanisms are also assessed.

The philosophy behind the SBA Check tool and this approach is *simplicity* and *efficiency*. The software tool will guide the user through the evaluation by asking a set of bespoke questions, each representing potential information security controls (countermeasures). The approach results in a snapshot view with regards to the information security situation in the analysed organisation. This approach also helps identify possible changes that would help reduce or eliminate identified weaknesses.

The difference between this approach and classical risk analysis is that in risk analysis the starting point is to identify *threat scenarios* that can negatively affect information assets. Then one tries to establish the probability for a scenario to materialise and its possible consequences in monetary terms. Once this is done countermeasures are identified to reduce the identified risk. Using the approach presented here, the starting point is diametrically opposite – it starts with a list of countermeasures (referred to as “controls”) that are generally accepted as best practice, and thus suitable for most organisations. By matching these controls against the organisation’s business needs and requirements, we end up

with a faster and more efficient evaluation approach. However, there are application areas where a classical risk analysis can be fruitfully used also within information security, but problems with *e.g. monetarizing risk* and *pricing information assets* and *discounting monetary flows to net present values* are often too great to make it a worthwhile exercise.

5.2.2 Overview of the approach

The evaluation approach entails three stages (figure 5.4):

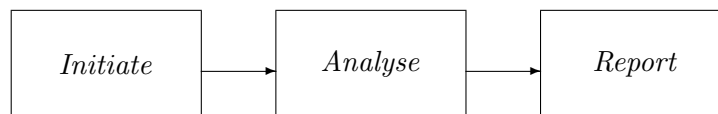


Figure 5.4: Overview of the evaluation process.

1. *Initiate*: Set-up the evaluation
2. *Analyse*: Gather information and perform evaluation
3. *Report*: Communicate the findings

The following sections will describe each of these stages in turn, and conclude with a discussion about the presented evaluation approach and the associated software tool.

5.2.3 Stage 1: Initiate

Objective: To build a solid foundation for the evaluation process resulting in a documented evaluation plan and agreement. Figure 5.5 shows an overview of the initiation stage.

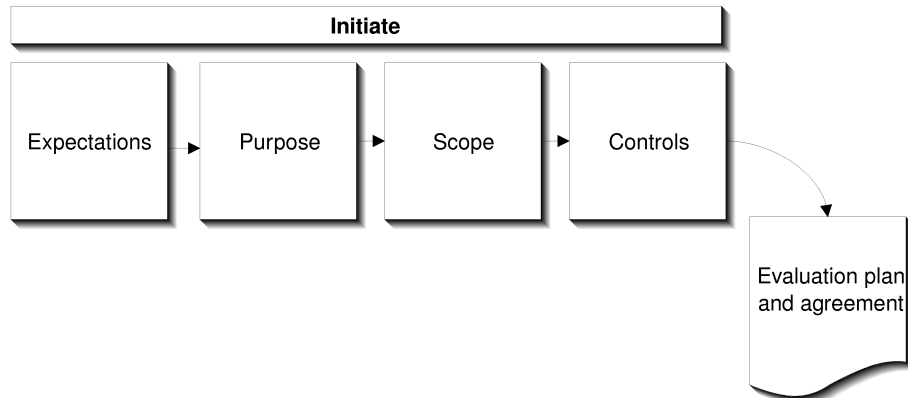


Figure 5.5: Overview of the initiation stage.

Expectations

One of the most important issues is to identify stakeholders' (clients' or other benefactors') expectations with regards to the evaluation results as early and as accurately as possible. By identifying and co-developing these expectations at the onset of the evaluation, the result is more likely to be perceived as valuable and useful. The ideal method for identifying and co-developing expectations differs from situation to situation. However, a meeting in person with important stakeholders to discuss the impending evaluation has proved to be a very efficient way to clear out any misunderstandings and to identify and discuss any implicit and explicit expectations. Expectations can relate to all aspects of the evaluation (figure 5.6).

Action point: Stakeholder expectations should if possible be agreed on and documented in the evaluation plan and agreement.

Purpose

The purpose of the evaluation should also be established at an early stage, since this will determine how the evaluation ideally should be



Figure 5.6: Example of expectations on the evaluation.

conducted. The core questions here are:

- *Who* will be the recipient(s) of the evaluation results?
- *How* and for *what* are they planning to use the findings?

Information gathered and analysed in the evaluation process must be in line with the overall purpose of the evaluation. For instance, the purpose governs the required accuracy and precision with which the questions ideally should be answered, and if any kind of verification is required or not.

Example – *purpose* and *implications* for the evaluation process:

- A client asks for an SBA Check evaluation of the information security situation in the organisation.
- The purpose is to *identify current deficiencies* and to *pinpoint solutions* that could be implemented to solve these deficiencies.

- Therefore, potential improvements will have to be documented with extra details, so that the evaluation result can be used as input in the decision situation when the client is going to decide on which countermeasures to implement.

Action point: Document the purpose of the evaluation in the evaluation plan and agreement.

Scope

The scope of the evaluation should be established to ensure that the evaluation really analyses the decided unit of analysis. This is especially crucial if the evaluation result is to be used as a basis for certification according to some information security standard such as ISO/IEC 17799 ISO (2000). Some common delimitations of scope include:

- Which IT systems and communication networks should be included in the evaluation? (Only those in-house or also outsourced?)
- Which parts of the organisation should be included in the evaluation? (Which geographical, juridical, or functional units? Only the head office? Subsidiaries?)

In large organisations, for example, it is common to conduct multiple small evaluations on organisational units and then compile the findings.

Action point: Document the scope of the evaluation in the evaluation plan and agreement.

Controls

The final activity of the initiation stage is to establish the *set of controls* to perform the evaluation against. The choice of controls depends on all of the three previous activities (expectations, purpose and scope). This is essentially choosing which checklist to use for the evaluation at hand. SBA Check is delivered with three sets of controls:

- Check
- ISO/IEC 17799
- FA22

In short, *Check* was developed by the Swedish Information processing Society via leading information security experts in Sweden, ISO/IEC 17799 contains all the controls listed in the international standard, and FA 22 contains all controls related to the rules about computer systems security as stated in the Swedish regulation *Beredskapsförordningen* clause 22. This regulation is only applicable to society-critical systems, but may still be of interest for some evaluators.

Most evaluators are likely to choose to evaluate against either the ‘*check*’ set of controls or ISO/IEC 17799, as they represent Swedish and international “best practice” (respectively) for information security management. However, it is also possible to adopt a different set of controls to evaluate against, as there is support for this in the SBA Check software.

Action point: Record the choice of controls in the evaluation plan and agreement.

Evaluation plan and agreement

Stakeholders’ expectations, evaluation purpose and scope, and the selection of controls are now established. All of these should be documented in an evaluation plan and agreement (Figure 5.7). The objective with such a document is:

- To ensure that stakeholders have a good grasp of what they can expect with regards to the evaluation results,
- To ensure that all individuals involved in the evaluation in any way understand its purpose and scope if required,

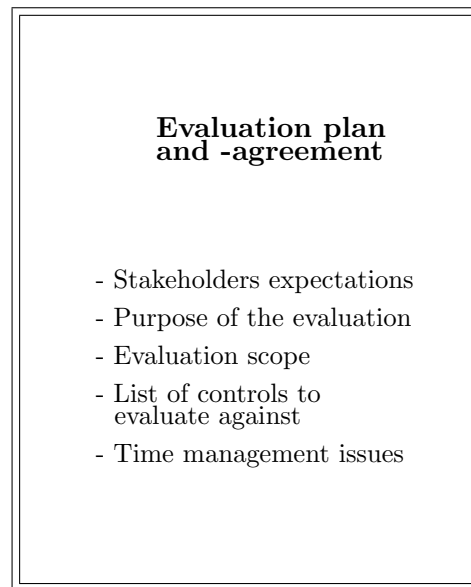


Figure 5.7: Typical contents of an evaluation plan and agreement.

- To help the evaluator to focus on the agreed scope during the evaluation process, and
- To aid the evaluator's and stakeholders' recollections in any discussions and potential future disagreements about the evaluation after it has taken place.

5.2.4 Stage 2: Analyse

Objective: To gather and analyse information about the information security situation under examination, aiming to arrive at a truthful view of the situation. This stage, as described here (figure 5.8), is to be executed once for each question (representing a control).

Examine question to determine evaluation strategy / Identify information sources: The first step is to read and understand the question asked by SBA Check. To further explore the meaning of

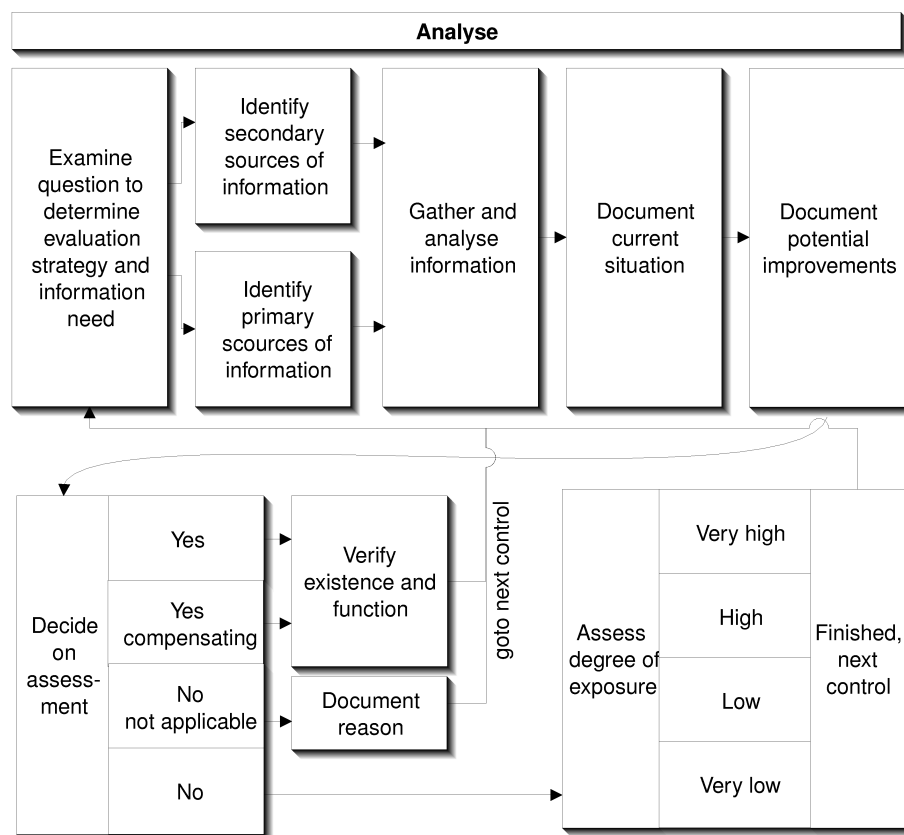


Figure 5.8: Analysis stage.

the question, one can refer to the “best practice” description for each question. The nature of the question determines the ideal evaluation strategy, and the information sources needed for the evaluation. For example, if the question is regarding a technical control, one might have to consult system utilities to gather information from IT systems. If the question is regarding the existence and function of some formal procedure, one might have to consult the organisation’s security handbook and interview those supposed to carry out that procedure.

Gather and analyse information: This stage can be very complex if dealing with a large or geographically dispersed organisation, or if the IT systems are very complex and heterogeneous. Sampling is often necessary as it is not economically feasible to, for example, interview all users about their awareness of the information security policy.

Document current situation / Document potential improvements: Once information is gathered and analysed, the current situation with regards to the control at hand can be documented in the software tool. Details of the current situation might include, for example, references to existing information security documents and results of interviews. Potential improvements can be based on either the evaluators’ direct knowledge or be inspired by the best practices described in the tool.

Decide on assessment: There are four possible quantitative alternatives:

- *Yes*, control exists and functions adequately
- *Yes*, compensating control exists and functions adequately
- *No*, control not applicable for special reason
- *No*, control does not exist or does not function adequately

What is adequate is a multi-dimensional judgment – it depends on the organisation’s business, its reliance on information and IT systems, and the perceived efficiency (costs and benefits) of the installed control.

Verify existence and function: If one of the first two alternatives is chosen, one can optionally document if any verification of this has been done, such as a real technical test, or if the assessment is based on, for example, hearsay.

Document reason for non-applicability: If the third alternative is chosen – “No, control not applicable for special reason”, then this reason must be documented. For example, a question about a firewall protecting the organisation from threats via the Internet might not be applicable to organisations and systems that are not connected to the Internet at all.

Assess degree of exposure: If the fourth alternative is chosen, it means that some kind of weakness is identified. In these cases, one can assess the degree of exposure on a scale ranging from “very low” via “low” and “high” to “very high”.

Finished: This was the whole process for each control, so now one can start over again with the next control in line. An average evaluation contains circa 100 or so controls, depending on the established set of controls to evaluate against.

5.2.5 Stage 3: Report

One of the ideas behind a tool like SBA Check is the capability of automatic reporting at the end of the evaluation. The report generator can sort the evaluation result according to any criteria, including degree of exposure (to see the vulnerabilities with very high risk first), assessment decision (to see e.g. all controls that failed at all). In addition, graphical reports can be generated with statistics of how the organisation is doing in different areas of information security.

It is imperative to communicate the findings in person to evaluation stakeholders, and also to think about the need to keep evaluation results confidential where required.

5.2.6 Discussion and limitations

The tool and methodology's role in this research

At this stage, SBA Check and the evaluation approach presented in this chapter can be seen as hypotheses. So far, we have not formally evaluated the use of SBA Check. This should therefore be viewed as one way of conducting this type of evaluation.

Evaluation of the evaluation tool and approach

The formal evaluation from a user perspective of the tool is in the design phase right now. This evaluation will be carried out by means of a survey of all licensed users of the tool. However, the tool is *informally* tested in two ways already:

1. At courses held by the author of this thesis for information security managers: Circa 100 information security managers and consultants have been attending 2-day courses about the proposed tool and its practical use. The entire course was designed and carried out by the author of this thesis. Each *course* was evaluated using surveys, and the results were very good. In the last course held, 100% of the participants evaluated the course as “good” or “very good”. Although this evaluation was not about the evaluation approach directly, it can be seen as indicative of the value of the approach since the course was focusing on this.
2. At real evaluations in Swedish and International organisations: Circa 200 licensed users of SBA Check use the tool to evaluate the information security in organisations. Again, this does not mean that the method and tool are good, but it is at least an indication that organisations are eager to use it.

Limitations to the tool and evaluation approach

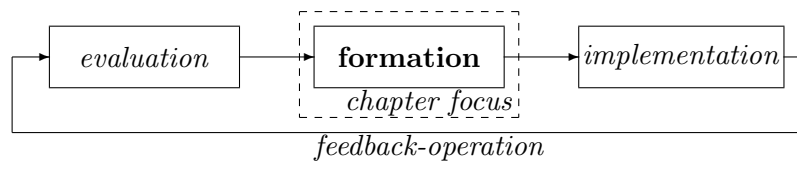
When choosing to evaluate information security in one way, that choice also means other ways are *not* chosen. Each software tool and approach to evaluation has its benefits, but also its negative sides. These are the most important limitations to this approach:

Cost-benefit analysis not supported. In SBA Check, monetary values are left out, so there is no way to analyse the potential costs and benefits of an existing or suggested information security control. As an alternative, the decision of judging a control as adequate or not entails considering the financial impacts on a high level.

Checklist-based approach. Approaches based on formalized checklists are often, and rightly so, criticized for the inflexibility and rigidity inherent in the approach. For example, a risk or a threat scenario that would require some security measures to be considered that is not included in the set of controls listed in the checklist (or in the evaluation database as in SBA Check) cannot be identified and dealt with. Therefore serious threats, critics argue, might be overlooked. This is one major weakness of SBA Check and the evaluation approach described here. To minimize the effect of this weakness, we have taken the following measures:

- *A variety of checklists:* Three different checklists are included in SBA Check, each of which is tailor-made for a specific purpose (for example, one for information security management evaluations and one more focused on IT systems security)
- *Open structure:* Third party developers can develop and market checklists for specific purposes (*e.g.* a specific Windows XP checklist could be used for security evaluation of an XP based computer network)
- *End-user flexibility:* Each user can, via an editor built into the software tool, amend the checklists to suit their environment, organisation, culture, legal system, IT infrastructure, *etc.*

In this way, we have at least reduced the effects of these serious weaknesses of checklist-based approaches.



Chapter 6

Formation stage - Paper B: “Creating ISMS - A Study of Success Factors”

This paper presents the findings of an empirical study of certification auditors' and information security consultants' experiences and insights concerning the formation and certification of information security management systems ¹. The original title of the paper was "Implementing Information Security Management Systems - An Empirical Study of Critical Success Factors". Using an action research inspired strategy and a Grounded Theory-like research method, the study describes these particular experiences and insights primarily in terms of success factors vital to the formation and certification processes. Two tentative theoretical frameworks, providing synthesized views of these factors, are put forth.

¹This chapter is based on a previously published research paper (Björck, 2001a)

6.1 Introduction

6.1.1 Related work

Formation and certification of ISMS (information security management systems) currently interests many researchers and practitioners. Especially 7799 – the British and now also international standard for ISMS (ISO, 2000; British Standards Institute, 1999) - have received a lot of attention in the information security research community lately:

Siponen (2001) criticises 7799, and other information security (management) standards, from the viewpoint of philosophy of science and argues that these standards were developed based on personal observations that were not scientifically justified. In addition, Siponen argues, the standards in question claim to be universally valid, although they are not.

Eloff and von Solms (1998, 2000b,a) suggests that both IT product security (measured by for example Common Criteria) as well as procedural information security (measured against for example 7799) have to be taken into account when measuring the level of information security in an organisation.

Von Solms (2000) declares that information security must be managed on both a macro and a micro level. The macro level (information security at an inter-organisational level) should be managed with the help of, and measured against, an internationally accepted framework, such as the 7799 standard. The micro level (information security at the intra-organisational level) should be managed through a dynamic measurement system. Furthermore, he argues that an information security certification scheme, such as that set up for 7799, should play an important role in the future.

R. Von Solms makes a business case for the standard using a metaphor of driving a car:

“Any motor vehicle on a public road requires a valid roadworthy certificate that will indicate that all technical safety and

security mechanisms and features on the vehicle are present and functioning properly. The driver needs a driving licence that will indicate that he/she has learned how to drive the vehicle in a secure way by using the technical safety features correctly and effectively. Further, a third party, i.e. traffic officers, will continuously ensure that the vehicle is functioning technically well and also that the driver obeys all road usage regulations.” (Von Solms, 1999)

He concludes, “. . . BS7799 can certainly provide the basis to ensure “safe driving on the information super highway” (Von Solms, 1999).

Labuschagne (2001) asserts that 7799 could rightfully be used as one of the cornerstones of web assurance in an electronic commerce context.

6.1.2 Justification for an empirical study

Although much has been written about the standard itself, very little has been written about the *practical application* of the standard. And so far, we have not found any published empirical studies on this subject – at least not related to the 7799 standard. Consequently, even though this study is somewhat limited in its scope and depth, it might still prove interesting for practitioners and academics.

6.1.3 Research question

The research question of this study is:

What are the success factors to consider while creating a management system for information security?

6.2 Research method

6.2.1 Research strategy

The high-level research strategy within which this study was carried out can be labeled a modified action research strategy. This strategy is portrayed, and the *rationale* for choosing it is explained, in chapter 3 of this thesis.

6.2.2 Data collection method

Two sets of questionnaires were developed and sent to the respondents. They were composed of open-ended questions, so as to not restrain the thinking of the respondents. Each form contained six questions, and they were slightly different for certification auditors and information security consultants. This paper only reports the findings of one question, which was posed in exactly the same wording to both groups²:

In your opinion, which are the critical success factors for a successful implementation of an information security management system, ISMS? (Please give reasons for your answer)

Let us comment briefly on three aspects with regards to the wording of the question above:

- The questionnaires were written in Swedish, so this is a translation.
- Although the question does not explicitly refer to the standard as such and to the problems associated with the certification process, the respondents rightly read this into the question because of the context within which it was asked. That context is: that they were asked about their experiences and insights as members of the Swedish 7799 pilot certification group.

²The two original reports of this study, which reports on *all six questions* is available in Swedish, and included as appendices B and C

- The question uses the term implementation in a broad sense, which differs somewhat from the meaning we give to the term in the ISMS framework in this thesis (in chapter 4). Here, the term encompasses all of the activities in the ISMS framework, while the *focus is on the formation stage*. The reason for writing this explicitly here is only to clarify why the question in this chapter reads “implementation”, while the results of the collected materials, and most of this chapter, focus on problems and success factors related to the creation of management systems for information security (*i.e.* the formation stage).

In total, there are 8 certification auditors and 18 information security consultants in the Swedish 7799 pilot certification group, which makes up the total population. All of these were asked to complete the questionnaire, so we did not need to make a random sampling in this case. The response rate for the certification auditors was 75% ($(6/8)*100$), and for the consultants 72% ($(13/18)*100$). We have not formally analysed why some decided not to answer the survey. However, we do know that most of the ones who have not answered are new members of the group. Being new, they are likely to have limited experience and insights about the exact question. This fact might explain why they did not answer.

6.2.3 Data analysis method

The data analysis method employed is inspired by the ideas of Glaser (1978, 1992, 1998) and his view of Grounded Theory. However, one significant difference between the adopted data collection and analysis method and the Glaserian view of Grounded Theory is that we have not employed theoretical sampling (meaning to let initial findings in collected data direct further data collection), since the data was collected in one go using questionnaires.

The answers ranged from single sentences to quite extensive explana-

tions. The exact answers were imported into ATLAS/ti, a methodology support tool for qualitative analysis of data especially supporting qualitative data analysis (Muhr, 2004). In line with the ideas of grounded theory, analysis was conducted without any pre-determined categories.

First, each answer, for example a sentence, was coded with a code describing its content. Second, patterns were looked for in the data material by comparing the codes from the first stage. These patterns gave rise to new codes, or in these cases categories.

Figure 6.1 illustrates the codes and categories found when analysing the empirical material gathered from the information security consultants. Each individual quote behind each code is *not* shown here. Instead, there is a number in each box indicating the amount of quotes supporting (or rather "forming") each code/category (figure 6.1).

Categories were created based on the following criteria (Guba, 1978):

- *Internal convergence*: codes grouped in a more general category should be semantically related to each other.
- *External divergence*: categories formed should be semantically separate from each other.

Of course, the researchers' pre-understanding of the phenomena will affect the process and the result of data analysis. However, this would have been no different even if there would have been pre-determined categories in the data analysis phase.

The answers from the auditors and the consultants were analysed separately, and therefore will also be presented separately in this paper. The idea was to see if there were any differences in insights and experiences (and views) between these two groups.

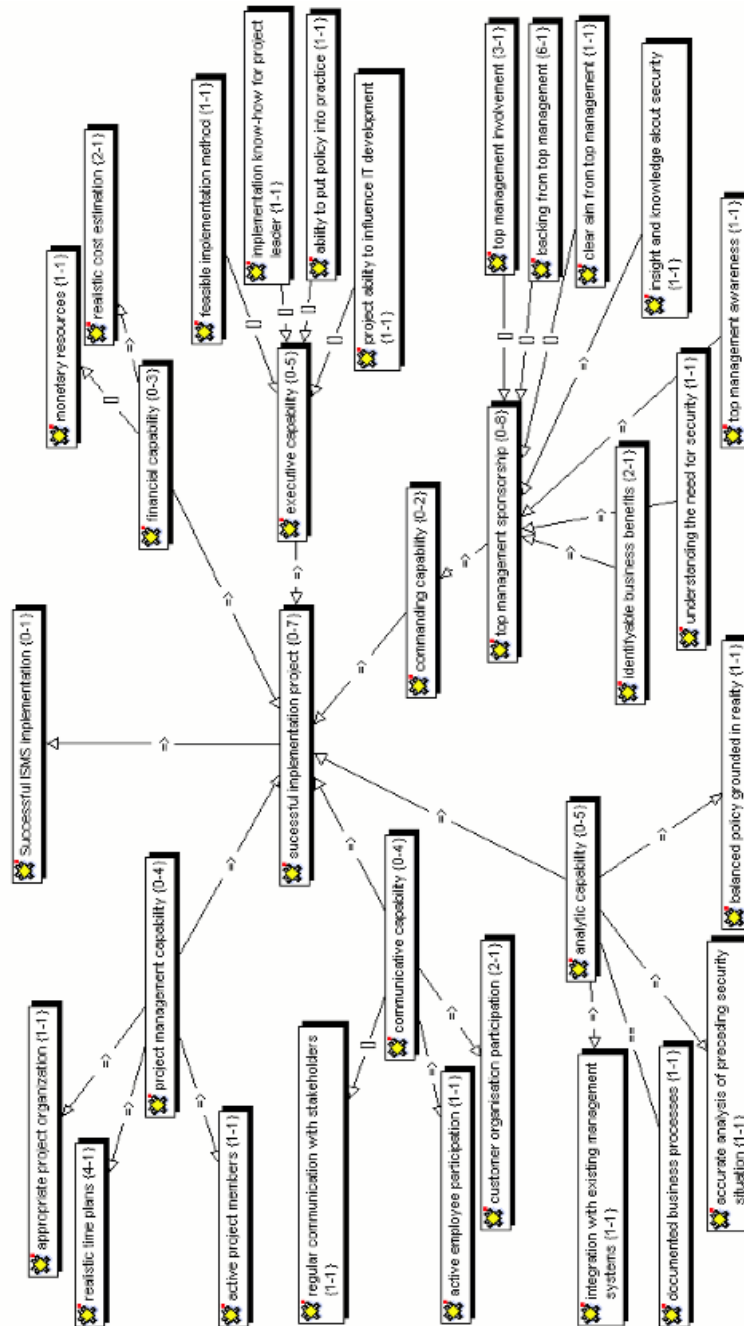


Figure 6.1: Illustration of how the empirical materials from the consultants are conceptually generalised – from single quotes via codes to categories - to form the theoretical framework - the success factors.

6.3 Certification auditors' perspective on formation and certification of ISMS

Once again, the question was stated as follows (translation from Swedish to English):

In your opinion, what are the critical success factors for a successful implementation of an information security management system, ISMS? (Please give reasons for your answer)

From the answers, we could distinguish six different success factors. Since the consensus was so profound, we chose to present the answers sorted after each factor, starting with the most important, or at least the most frequently mentioned factor. All the answers fell within these six categories.

The success factors for formation and certification, from the perspective of the certification auditors, were the following:

6.3.1 Management commitment

Support from the top management of the organisation, and their commitment to and understanding of the problems of information security was seen as one of the most important success factors for an efficient formation of ISMS. This factor was mentioned firstly by all of the respondents in this group (auditors), even though there were no fixed answer alternatives and despite the fact that the respondents were unaware of each other's answers. The following quotations speak for themselves:

"Top management's interest and commitment in its own ISMS project. ..."

"Top management's commitment and an understanding that the management system for information security must cover the whole business."

"Top management's commitment ..."

“Top management’s understanding and commitment, in deciding the security policy / security level and to participate actively in the risk analysis and the continuity planning.”

“Top management’s commitment. . . .”

“Endorsement from the company’s / organisation’s top management. . . .”

6.3.2 Well-structured project

Another important success factor which was identified was that the ISMS formation project in the organisation is well planned and structured. The respondents expressed it like this:

“An organisational unit responsible for the totality and for the risk analysis which is the foundation for all activities. . . .”

“... a well defined project with delimited sub-projects . . .”

“A well developed project plan and a correctly dimensioned project organisation. . . .”

Taken together, there are many aspects concerning the organisation of the ISMS development and implementation that are mentioned:

- that the responsibility for the project is defined,
- that it is clear who shall carry out the different steps in the project
- that goals, resources and the time plan for the project are developed and documented in a project description, and
- that the resources in the project are well balanced.

6.3.3 Holistic approach

The project members' – and other employees' – ability to see the “full picture” is stressed by many of the respondents as an important success factor. Sometimes, it seems like the certification auditors have a feeling that the IT-technical aspects are handled in a very detailed way, but at the price of making it more difficult to obtain a holistic view. Therefore, they meant that a more holistic approach and thinking in the projects should lead to positive consequences and pave the way to a more successful formation and possibly certification of ISMS. Two of the respondents put it this way:

“...that the participants in the work with identifying the risks are representing the whole business, not only security but also other parts of the business.”

“Understanding that the management system for information security must cover the whole enterprise.”

As can be seen from the quotations, it is mainly the connection between the information security and the organisation's core activities (processes) that is seen as important – that the ISMS does take into account and that it covers the whole organisation – so that the ISMS does not end at the security or IT departments.

6.3.4 Appreciating the need for information security

That the organisations understand the need for information security is another success factor that was identified:

“...that the company becomes aware of a need to protect its own, its customers and other stakeholders' information.”

“...understanding that the management system for information security must cover the whole organisation”

“management's understanding...”

Although this factor may seem trivial, it is mentioned many times by the respondents. They sometimes perceive a lack of appreciation for the importance of information security from parts of the organisation.

6.3.5 Motivated employees

Some of the answers focused on the need to motivate employees:

"To motivate the employees to develop processes and procedures within their own areas of responsibility...."

"...motivated project management /-participants...."

The answers focus on the motivation of individuals participating in the ISMS project, such as project participants, project managers, and those responsible for different areas in the organisation. After the development of the ISMS, it will also have to be implemented, and at that stage the importance of this success factor grow – at that time, all employees in the whole organisation will have to be motivated to adhere to the rules. Further, they should regularly use the technical solutions that the projects have developed and the management decided on – they need motivation.

6.3.6 Access to external competence

The final success factor identified by the questionnaires was the importance of being able to call for external competence when needed:

"...good reference persons (preferably certification authorities from the beginning)."

"... access to external specialist competence."

This factor is concerned with both experts and advisors in IT- and information security, but also about opening the dialog between the organisation and the certification authority at an early stage. This contact – organisation vs. certification authority – must be seen as very important

– at least if the organisation is planning to seek certification of its ISMS after the implementation.

6.3.7 Summary

The certification auditors in the Swedish pilot certification group viewed these six factors as critical for the successful formation and certification of ISMS (figure 6.2):

- Holistic approach
- Motivated employees
- Well-structured project
- Awareness of the need for security
- Top management's commitment
- Access to external competence

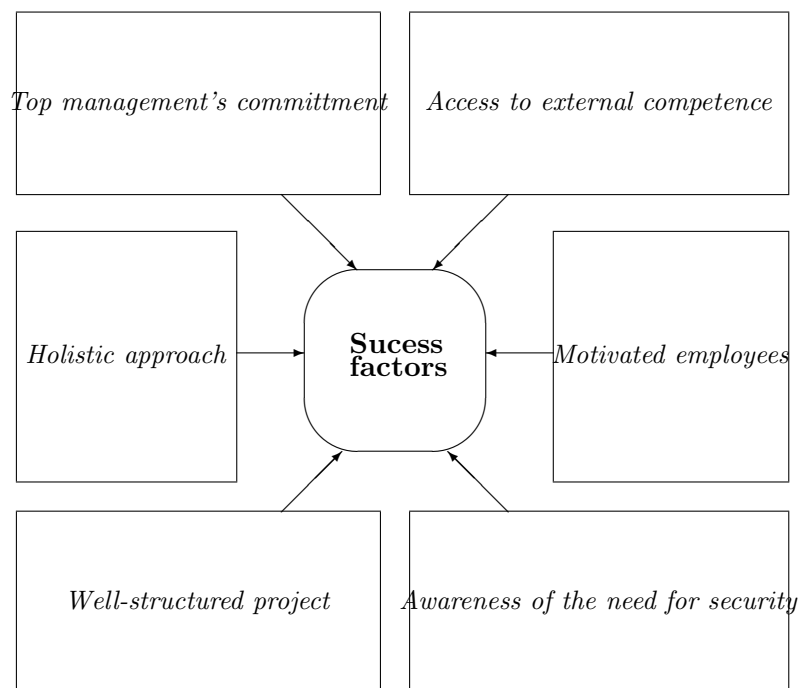


Figure 6.2: Success Factors for the formation and certification of information security management systems, from the certification auditors' perspective.

6.4 Information security consultants' perspective on formation and certification of ISMS

Also for this group, the question was stated as follows (translation from Swedish to English):

In your opinion, what are the critical success factors for a successful implementation of an information security management system, ISMS? (Please give reasons for your answer)

Also here, the answers were analysed using a grounded theory method supported by a computerized data analysis tool (ATLAS/ti).

In total, there were 37 quotations from the consultants on this question. They were first analysed and coded into 23 different categories, using no predetermined codes. This means that the essence of each quote can be represented by its code on this level. Afterwards, these 23 categories were further analysed using the qualitative data analysis tool and we found that they fell into 6 more abstract categories.

Even though all the answers were in Swedish, we decided to code each quotation in English, so that they would be easier to present in this paper. However, the answers were not translated, but they are available in the Swedish report for those interested (see appendices B and C of this thesis).

It should be noted that there is no logic in the data analysis tool to help decide on the categories of the data. The tool is only used to organise the analysis, and to keep track of and visualize the analysis result.

Here are all the codes used at the first level of analysis (in alphabetical order):

1. ability to put policy into practice
2. accurate analysis of preceding security situation
3. active employee participation

4. active project members
5. appropriate project organisation
6. backing from top management
7. balanced policy grounded in reality
8. clear aim from top management
9. customer organisation participation
10. documented business processes
11. feasible implementation method
12. identifiable business benefits
13. implementation know-how for project leader
14. insight and knowledge about security
15. integration with existing management systems
16. monetary resources
17. project ability to influence IT development
18. realistic cost estimation
19. realistic time plans
20. regular communication with stakeholders
21. top management awareness
22. top management involvement
23. understanding the need for security

These codes were further analysed and categorized into six more abstract categories. These six categories were:

1. Project management capability
2. Commanding capability
3. Financial capability
4. Analytic capability
5. Communicative capability
6. Executive capability

These capabilities form the foundation for a theoretical framework. Here is a short description of each of these capabilities.

6.4.1 Project management capability

A successful implementation project will need to have efficient project management capability. This means for example that for active project members, an appropriate project organisation and realistic time plans are needed.

6.4.2 Commanding capability

The commanding capability stems from the top management sponsorship of the project. It is this capability that gives the project the authority to decide on issues regarding information security. Without any real decision making power, it is very hard if not impossible to achieve the project goals. This capability is given by for example top management awareness and involvement in information security, identifiable business benefits and an understanding for the need of security, and a clear aim and backing from top management.

6.4.3 Financial capability

All information security projects need budgeted resources. A project with this capability is able to estimate costs realistically. It also has

access to the resources needed to carry out the project.

6.4.4 Analytic capability

Projects with analytic capability can accurately analyse the preceding security situation, and therefore develop a well-balanced ISMS which is also integrated with existing management systems (e.g. quality and environment management systems – iso900X and iso1400X). In short, this capability is needed to create a balanced policy grounded in reality.

6.4.5 Communicative capability

Many information security efforts stop at the security managers' desk. To avoid this, a communicative capability is needed. This capability is needed to enable regular communication with stakeholders and for active employee participation in the project.

6.4.6 Executive capability

Thinking about security and writing policies is one thing; implementing the ideas, rules, controls, and procedures is another. The executive capability means that the project can do things – that it can make things happen. One of the things that will need to be done is to put the policy into practice and this in turn often requires for example the ability to influence people in the IT department, in IT development and in other parts of the organisation. A feasible implementation method and implementation know-how for the project leader are examples of parts that form this capability.

6.4.7 Summary

The information security consultants of the Swedish pilot certification group viewed these six capabilities as critical for the successful formation and certification of ISMS (figure 6.3):

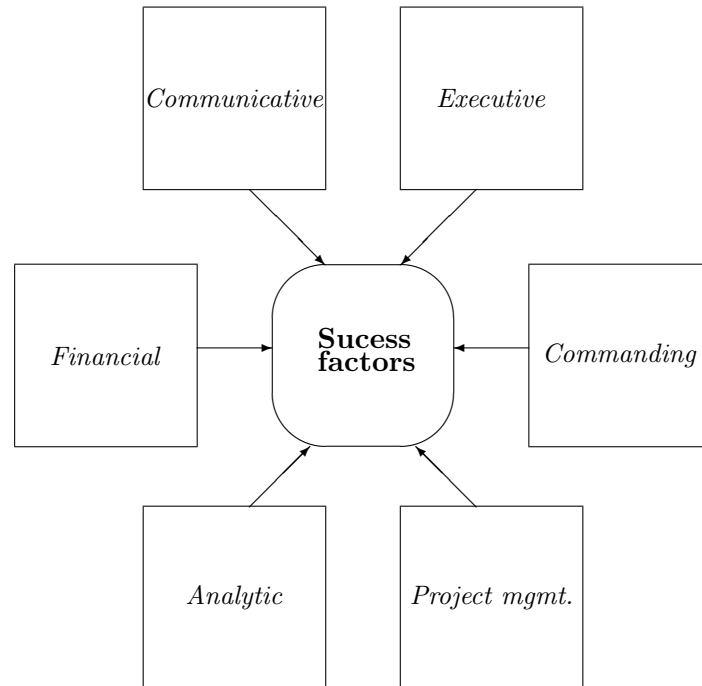
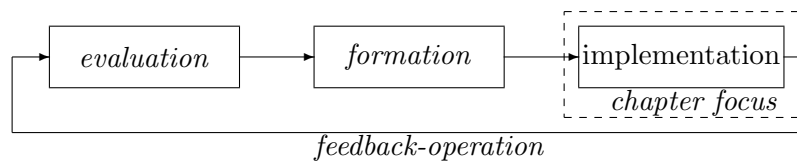


Figure 6.3: Success Factors, expressed as project capabilities needed, for the formation and certification of information security management systems, from the information security consultants' perspective.

- Financial
- Commanding
- Analytic
- Project management
- Executive
- Communicative

6.5 Conclusions

Using an action research inspired strategy and a grounded theory like research method, this study has identified success factors for the formation and certification of information security management systems. Even though we cannot statistically generalize these findings to a broader population, we believe that these results can be useful and valid, especially for researchers and practitioners working with 7799 and similar management standards.



Chapter 7

Implementation stage - Paper C: “Value and Assessment of Infosec Education”

Information security education and training needs to be valued and assessed from various perspectives. This study presents two differing viewpoints from which such an evaluation can be perceived – those of the individual and the organisation¹. Some sort of profits are sought after by each of the two, although this is expressed and hence valued differently depending on the perspective taken. From the organisations’ point of view, training and education are key activities while implementing information security management systems. In that respect, this paper illuminates some critical issues related to the implementation stage, in which the effectiveness of information security education and training

¹This chapter is based on a previously published research paper (Yngström and Björck, 1998). Section 7.1 of this paper is co-authored with Yngström, while section 7.2 is entirely written by Yngström but presented here for purposes of completeness. All other parts of the paper are authored by Björck.

can be viewed as a key performance indicator. In particular, the paper examines; the need, current techniques, and practical problems, related to measuring. The main purpose is to demonstrate the limitations of, and problems related to, current techniques employed when assessing the potential economic impact of information security training programmes.

7.1 Introduction

The Internet evangelium is rapidly embraced everywhere – log onto “The Net” and meet new friends, order that vegetarian pizza, place a phone-call, visit the Museum of Ancient Art, groove to the latest hit, watch the news, make business the modern way - go global! Undeniably, the potential benefits are immense. However, most of us forgot that all coins usually have two sides: “You can pay me now or you can pay me later”, as Murray (1995) phrases it. In the haste to get online, organisations and individuals alike have sometimes ignored information security risks. Hence, today the need for information security education and training is more evident than ever.

- The times when only a few experts needed education and training in information security are gone forever. Today journalists, politicians, managers, parents, pupils, teachers and other individuals require this type of knowledge.

- The times when the whole body of IT knowledge could fit into the finite domain of computer science are gone forever. Today ethical, social, legal and economic implications of IT use must be considered - so also within the realm of information security.

- The times when information security could be taught solely in a linear fashion focusing mainly on aspects of confidentiality are gone forever. Today the information security agenda has changed - aspects such as trustworthiness of information are seen as more important. Further, the new broadened curriculum demands new pedagogical tools – ideally interdisciplinary and holistic approaches.

As the conditions for information security education and training change, the need for thorough evaluations and assessments are on the rise. This study presents the need for information security education and training, the need for assessing (or measuring the effects of) such efforts, and some examples of methods and problems pertaining to assessment. These three aspects tend to look very different from the viewpoint of the organisation compared to that of the individual. This paper tries to capture these differences by presenting one section about information security education and training from the point of view of the individual and one section from the viewpoint of the organisation. The purpose is to demonstrate the limitations of, and problems related to, current techniques employed when assessing the potential economic impact of information security training programmes.

7.2 The individual's perspective

7.2.1 The value of and need for information security education and training

It is hardly possible to develop adequately secure IT systems and information management procedures unless high quality education and training in information security is available to individuals – system developers as well as users and others. The vast majority of all information security education and training efforts have been aimed at computer specialists, while other groups such as professional users from other disciplines as well as regular and casual users and usees have been overlooked. As a result, these computer specialists have provided the world with advanced information security models, methods, architectures, and tools. Unfortunately, many of these have proved to be insufficient or too complex to use. Consequently, the need to educate and train also other groups of individuals in the art of information security has recently been noticed. Selected arguments from these information security scholars reiterates and reinforces this belief:

Highland (1992) suggests that the failure to develop meaningful computer security practices have to be shared by three communities: The academic community which has been lax in acceptance of computer security, the business community which was unable to specify its needs, and the military establishments which have designed models unsuitable for the real world.

Cohen (1995) suggests historical reasons: the important constituents of the information protection domain were separated into the sub-fields of cryptography, computer security, fault tolerant computing, and software safety. Computer security covers leakage, fault tolerant computing covers accidental events, and special purpose systems cover selectively otherwise uncovered areas. Specifically, taken together these sub-fields do not cover the full range of in-

formation protection and security (*e.g.* disruption of services not attended to).

Parker (1995) argues that defining the elements of information security, as the preservation of confidentiality, integrity and availability is a dangerously oversimplified definition that has to be extended. This definition is not sufficiently comprehensive to protect information appropriately in all of its security aspects.

Fååk (1995) argues we are lacking awareness; we have a market with too many customers knowing neither what they want nor what they can get. There is no lack of basic tools but a severe lack of good implementations. Moreover, experts and practitioners are not interested in each other's questions, thus they do not communicate.

These statements should be taken seriously - lack of meaningful computer security practices, separation of the information protection domain into sub-areas, incomplete definitions, and inadequate awareness. They have in common that they mark the need for information security education and training, not only for computer specialists, but also for individuals in other positions. Moreover, these sceptical statements about information security imply that evaluations of today's education programmes and training efforts might be deficient.

7.2.2 The need for measuring

From the perspective of the individual/learner, there are several reasons why assessment of education and training efforts ought to be undertaken, *e.g.*:

- Existing education and training on various levels do not yet cover the full range of needs, even though there is a positive trend in numbers of courses offered by universities and other organisations. Through citing explicit areas for improvement, an assessment effort

may play a significant role in ensuring that future courses and academic programmes advance to be more comprehensive.

- Depending on their present stage in life, individuals might strive to get a job, to obtain a better position, to gain higher self-esteem, or to perform tasks at work more efficiently and effectively. In whatever situation the individual is in s/he is looking for knowledge that can make their life (or others) a little bit better – individuals want their knowledge to help them earn profits - not necessarily purely financial. Assessment of courses and programmes in information security can assure this in two ways: Firstly, assessment supports advancing and sustaining the quality of the knowledge that is delivered to the individual. Secondly, given that the assessment leads to a high quality course or programme, it will attract individuals eager to learn information security, which will further increase the quality.

The necessity to evaluate information security education and training is now apparent, although choosing the scope and the method of evaluation is not always as simple. The National Institute of Standards and Technology (Wilson et al., 1998) in their special publication on ‘Information Technology Security Training Requirements’ suggests that an assessment should cover the learner’s subjective satisfaction, the learning effectiveness, the teaching effectiveness, and the program effectiveness. For each of these four levels they describe three types of programmes: basics/literacy, training and education. This scheme covers aspects pertaining to the individual, the organisation and to some extent also societal aspects. In the following section we will present evaluations focusing the aspects of the individual and the pedagogical methodology. Even though the outcome of such an assessment depends on the students and teachers, organisations and societies later estimate the value of the education or training effort indirectly – on the job market.

7.2.3 Techniques for measuring – an example

General. Yngström developed a similar approach to evaluation as that suggested and described by NIST (Wilson et al., 1998), in Yngström (1988, 1989, 1991, 1993, 1996). This approach was used for evaluating an interdisciplinary and holistically oriented academic IT security programme. The evaluation also included assessment of a specific pedagogical methodology chosen to fit the interdisciplinary and holistic approach.

Background – evaluation setting. The educational programmes involved were initially two one-year programmes, one on undergraduate level (Bachelor) and one on graduate level (Master) at the Department of Computer and Systems Sciences (at Stockholm University / Royal Institute of Technology in Stockholm, Sweden), in what became labeled the "Security Informatics Programmes". These programmes were later split into smaller units which also were involved in the evaluations. Also an evaluation of a single IT security course including the pedagogical methodology, offered in a non-European university environment was included. The development of programmes and their courses began out of need and curiosity. The Swedish Vulnerability Board had recommended all educational institutions, including universities, initiate courses in (then) EDP security, and practical circumstances made us hypothesise that a specific pedagogical methodology using system theories would be a useful vehicle to understand interactions between technical and non-technical components needed for secure IT environments. The courses were originally developed in interaction between members of the Vulnerability Board, industry and academia (Yngström, 1983). As an educator it is fundamental to see what happens. But how should such courses be evaluated, their main goal being to lessen vulnerability in trade, industry, government, and societies? It was quite clear from the beginning that the primary groups to be educated would be managers responsible for the enforcement and measures of safety and security in

computer systems at different levels of society and organisations. Therefore the initial target group for education was specified as managers, or managers-to-be, of security in organisations that use computers, and the intent was to increase the professionalism within these groups by providing them with a specialised undergraduate degree that would also qualify for entering graduate studies. The goals of the first programme on undergraduate level were stated as:

Of such an extension and be placed at such a level that width and depth, theoretically as well as practically, will bring the student ability to participate independently in the processes of planning, designing, implementing, evaluating systems and functions which will lead to the demands of reality for system survival capable of being realised. In this context the concept system does not only imply technical ones (like computer, communications) or administrative ones (information, surveillance) but the total reality including the artefacts needed to create stable and robust structures on different levels of society. (Yngström, 1983, : 297).

Early evaluations to refine the programme. The first evaluations were regular pedagogical ones, concerning aims and scopes, course structures, contents, levels, modes of presentation, literature, examinations, overall structure, acquired attitudes, conducts and abilities and involvement from industry. These were conducted annually from the beginning and used mainly to trim the programme. In these evaluations it also became interesting *vis-à-vis* the chosen target group to see how active and what specific activities outside the class room participants were involved in. This made us include various statistics in the evaluations such as previous experiences from traditional security or IT security, previous academic studies in various disciplines, memberships in professional associations concerned with IT security or other relevant areas, *etc.*

Evaluation of the use of system theory as a means of teaching.

Not until the courses and the programme had been found good enough - that is, when the students were happy with most of the aspects and could use the knowledge at work - was it time to investigate whether the original methodological idea of using system theories was of any use to them. This was in 1991 formulated into ten practical statements and presented to all students who had participated in the programme from its start five years earlier in 1986. The statements dealt with different aspects of the practical use of system theories: their contribution to the students' awareness of appropriate problems and their ability to deal with these, their contribution to students' abilities to work efficiently and effectively, and their contribution to the capability for continuous learning.

Design of the evaluation and evaluation questionnaires. The ten practical statements mentioned above were classified into three categories, and answers were marked on a scale 1-5 ('1' meaning agreeing fully and '5' not agreeing at all). It was also possible to answer 'question not relevant to me'. In order to know something about the market's opinion of these former students' abilities and knowledge in the area, questionnaires also asked for evidence of promotions and positions before and after the programme. By this time, about one third of the former students were professionals in the traditional security and IT security industries, a small group for which promotions and activities it was possible to keep track of even manually at this time. In parallel statistics were also kept of students' backgrounds, memberships, etc. This group of former students formed the Swedish Association for Information Security (SAIS) to promote further academic education in the area. A top priority was to increase the number of courses, and this became the embryo of the Master programme in Security Informatics, for which separate courses initially were given within the PhD programme of the same academic department. The evaluation design

of the first run of the Master programme in 1993/94 shows similarities with the very first evaluations of the Bachelor programme in 1986/87, the aim being to find out whether the programme met the needs of the students and the market and to trim it into a scientifically and pedagogically esteemed programme. The demands for knowledge in the area changed and widened during the time the two programmes have existed; regular bachelor and master students in Computer and Systems Sciences demanded to take some Security Informatics courses during their last academic year. This made the Department divide the Security Informatics programme into four units, of which three are units of two courses, each which may be chosen by regular students. This change became evident in the evaluations of 1992-94, where the usefulness of the pedagogical approach was investigated in the same way as in 1991, but this time directly after the students had finished the first unit. Many of these students had not yet started their careers and could only react to statements concerning the approach's contribution to their general abilities to handle IT security. The general statistics were also collected for further comparisons. Since the specific methodology as such is strongly influenced by the North European movements of participatory design and Soft Systems Methodology, we were specifically interested to know how the approach would be rated in a non-European culture. Therefore the 1992-94 evaluations include reactions to the statements also from one Australian group of honour students. This group was however fairly small.

Evaluation results. The results from the 1991 study were summarised as follows:

When it came to the assessment of whether the methodology chosen contributed positively to this group's ability of problem awareness, work efficiency and effectiveness and continuous learning, 92% agreed concurred. In agreement to at least 50 % were the 50 professionals within the secu-

rity area. The approach contributed the most to a person's ability to delimit and specify her own problems and work tasks, but also to her ability to specify for others, such as colleagues. Relatively high scores were attributed to specifying criteria for security products, to work efficiency and learning about new products, methods and facts. The contributions to the ability of working with new products and controlling the work of consultants scored the lowest. However, with a mean score of 45.9 persons being positive to all ten statements, the chosen methodology is perceived to have contributed to these people's ability to cope with traditional security and IT security.

The result of the 1992-94 studies were summarised as follows:

The low frequency of practical experiences in security and IT security made it impossible for the students to answer half of the statements, and also to compare reactions to all ten of them. Still, answers not referring to work experiences show high appreciation: in all the mean positive reaction to these five is 46.8 out of 60. For statements requiring work experience the positive mean was 7.6 out of 11. Based on the means, 78% were positive to the non working related statements and 69% to the working related ones.

A comparison between answers given by Australian and Swedish students was interesting but results were inconclusive. Swedish answers by all - practitioners and students - were higher rated than the Australian answers and there were no particular similarities in the individual ordering of the answers between the Swedish and the Australian students. When comparing the answers between Swedish and Australian practitioners, they varied more positively in different statements.

Comparison and analysis of the different evaluation results.

A special analysis of the results of the 1991 and 1992-94 studies was made, where answers were weighted in order to be able to compare them. This analysis showed that that the approach helps in forming personal learning models and acquiring good insights; and best for Swedish university students, second best for Swedish professionals, and thirdly for Australian university students. However, we do not find it reasonable based on such small groups to predict where the approach works best. The differences in duration of presentation, possibilities to try in practise and other factors were too large, in addition to the small size of the Australian group. Judging the figures in total may at least be used as an indication, pointing to the positive reactions favour in total used pedagogical methodology. It may be reasonable to interpret the result as the Systemic-Holistic Approach and the Systemic Module facilitate individuals to assess and understand problems, increase work efficiency (doing things right) and effectiveness (doing the right things) and foster continuous learning within the field of security and IT security - provided the student has some own experience to refer to. When students do not have their own work experience, Systemic-Holistic Approach and the SM still facilitate assessment and understanding of problems, increase of effectiveness (doing the right things) and fostering of continuous learning - but in order to also increase efficiency (doing things right) practice is needed. Assessment of the Master Programme included a question of where and if the approach had been useful. Eight of the eleven students noted "in all courses", and the other three offered varying but positive answers. In addition all students rated the programme as a whole to have fulfilled their different educational goals positively, giving a mean of 89% of the successful students. We would regard that as qualitatively very good answers; the organisation and presentation of the content had been more than satisfying to all participants even despite different educational goals. Also the Master programme has been shown to be efficient within the market for its successful participants: participants

	1987	1991	1992-1994	1993-1994
Population (N)	72	155	120	26
Answers (n)	72	71	60	11
Professionals in (IT) security	47%	70%	18%	91%
Pros. in other positions	60%	10%	38%	9%
Mean age	33	34	30	32
Women ratio	11%	13%	32%	9%
Academic success ratio	81%	46%	83%	46%
Educational background: CS	47%	70%	85%	100%
Educ. bgr.: BA, Econ. or Law	40%	51%	48%	100%
Satisfactn. pedagogical method	n/a	92%	69%pro 78%all	89%

Figure 7.1: Some general characteristics of the students

are satisfied with the programme and employers are happy to hire and promote them.

Figure 7.1 (table) was constructed in order to describe and discuss some other similarities and differences between the groups being evaluated in 1987, 1991, 1992-94 and 1993/94. Separate figures were taken from Yngström (1996, : 176) or compiled based on it. It is not the separate figures that are interesting, but they may reveal emerging trends:

Groups 1991 and 1993/94 are the most alike in professional attitudes and ambitions; they have a high percentage of traditional and IT security professionals with a low percentage of other professionals. At the same time the academic success rate in total of all starting students is below 50% for both groups. They also have in total the highest figures for the value of the Systemic-Holistic Approach and the Systemic Module. Other figures of interest to note are: fewer women seem to be engaged in groups with higher professional attitudes and ambitions, the age of professionals seems to be falling, and the group is totally well educated in more than one academic discipline.

The 1992-94 group was already earlier noted as a typical university

student group. It includes fewer professionals in traditional security and IT security. Members are younger, and also more women participate. The academic success rate is the highest of all groups. In total their appreciation of the SM and the S-HA is somewhat lower than the professional groups.

The 1987 group could be labeled 'old boys' not because of the low participation of women, but because it contained an enthusiastic first lot of varied practitioners with varied backgrounds and very strong wills to build good security foundations. Their academic success rate was as high as the student group although their theoretical backgrounds initially were lower than all other groups. Members of the 1987 group later on have moved into the 1991 group. Possibly the high percentage of professionals from other areas in 1987 have become professionals in traditional and IT security in 1991. Satisfaction rates with the Systemic-Holistic Approach and the Systemic Module are for 1991: 92%; 1992-94: 69% for statements answered only by professionals and 78% for statements answered by all, and 1993/94: 89%. Despite the fact that the groups as compared to each other they are quite different; 1987 being 'old boys', 1991 being IT security professionals, 1992-94 being regular university students, 1993 being a non-Swedish university group, and 1993/94 being a highly professional group, they all were in favour of the pedagogical methodology with satisfaction rates about 70-90%. It seems therefore reasonable to state that the methodology was useful to students of IT security. In addition, the strong involvement of professionals in the programmes showed that former students make good careers with increased salaries, high esteem and promotions, both as managers and specialists.

Scientific limitations of the evaluation approach. The presented example of evaluations is not claimed to be capable of generalisation in detail, and was not the intention at the time. However, the approach to evaluate the programmes on different levels as described by NIST (Wil-

son et al., 1998) was followed; student satisfaction with the courses in various aspects was evaluated, the learning effectiveness and efficiency were evaluated for performances within the education as well as performances and outcomes at the workplaces, and the long run effectiveness of the programmes were evaluated career-wise for former course participants.

These evaluations and comparisons were all carried out without using control groups, since at the time there were no comparable courses and programmes. Today it would be possible to use the same kind of evaluation tools: questionnaires, interviews, and inspections of examination and seminar-work results, for different courses and programmes. This would certainly, to students and educators, be of value for instance choice of institution or course revisions and developments. However, measuring the value in some sense of information security training and education, in the opinion of these authors, needs some standard or index to be measured against. In academic environments such standards exist, although they may vary from country to country, from university to university, or from one professional group to another. In the information security area for professionals, such standards also exist in various types - typically named certificates - initiated as a qualitative metric. We believe all such certificates, academic as well as professional, will be of use, but we also acknowledge that the area of information security is a moving target, hence a certificate will not suffice as a general measurement, but will have to be supplemented with something more, perhaps a form of index which will consider at least the age and content of the separate certificates. But not only is the area of information security a moving target, it is also partly a context-oriented issue: it is global in the sense of networking possibilities and it is local in the sense of existing social values and particular application areas. Such factors should probably also be weighted into an index.

This concludes the presentation of: the need, techniques, and practical problems related to measuring the effects of information security

education and training from the perspective of the individual. Now, let us have a look at the same issues but from the organisation's perspective.

7.3 The organisation's perspective

7.3.1 The value of and need for information security education and training

From the viewpoint of an organisation, information security not only promises to assist safeguarding information assets at a given cost but, more importantly, it can provide the organisation with a competitive advantage through lower costs and new business opportunities (e.g. Parker, 1997; Cresson Wood, 1991). Thus, organisations – from corporations through hospitals to government agencies – are increasingly becoming aware of the need to safeguard their information. At the organisational level, this is usually accomplished utilising technical as well as procedural measures – *all of which depend upon human behaviour and skills to perform*, for example:

- *Technical measures*: Installing, configuring and maintaining a secure Internet firewall will only succeed if the persons involved understand the elementary concepts of TCP/IP network traffic, have a good grasp of what inbound and outbound communications are needed, and are familiar with the interfaces used to accomplish the tasks at hand.
- *Procedural measures*: Handling information in the way described by an organisation's information classification scheme might require the understanding of how, for example, one uses the backup system on the office workstation and how one can positively verify the sender of a digitally signed document.

This fact – that the human factor is one of the most significant determinants of the overall success of information security efforts in an organisation – has been pointed out in several recent empirical studies on information security in organisations. The following quotes confirm this truth:

- Employees' information security awareness is perceived as the most important means to overcome security problems (Björck, 1998).
- According to RRV it is important that awareness of computer related crime and abuse is raised within the management structure of organisations. It should be a primary priority of management to work to reduce the risk and threat from the different kinds of computer crimes. These problems cannot simply be solved by acquiring more technology. (Riksrevisionsverket, 1997).
- "This study's main conclusion is that the respondents consider the main threat against the organisations' EDP stored information to be employees' unintentional and erroneous change and deletion." (Johansson and Kager, 1995).

By now it is evident that most organisations seem to need information security education and training and that they are likely to benefit from information security education and training efforts. However, organisations do not usually dedicate resources for projects with no measurable impact.

7.3.2 The need for measuring

Managers make organisational decisions in a way similar to the way most individuals make personal decisions: with bounded rationality. In an ideal world, this means they will try to reach the optimal decision from the viewpoint of the organisation's purpose, given the information available at the time of the decision. Decisions regarding investments in information security education and training are also likely to follow a similar decision process. Strategic decisions (those that have a considerable impact on the organisation) are usually approached in a more structured manner than less consequential operational or tactical decisions. Regardless of the importance of a given decision, some kind of cost-benefit analysis is always carried out before a decision is arrived

at – either implicitly or explicitly. Given that organisations have a finite amount of resources to employ in the pursuit of their missions, investments in information security education and training must compete against other possible investments. The actual decision process probably does not follow the logical path described here, since many decisions are arrived at for reasons other than purely rational ones (*e.g. political, power, etc.*). Nevertheless, these rational decision models are often brought forward before or after a decision to rationalise² a decision to be made or a decision already made.

7.3.3 Techniques for measuring – an example

A simplified example serves as an illustration on how organisations generally rationalize decisions regarding investments:

A manufacturer of studio quality microphones has 100,000 Euros reserved for investments in a given period of time. There are many different areas in the organisation that would benefit from new investments, such as a new microphone assembly machine. In addition, there is a need for a comprehensive information security education and training programme. However, the monetary resources will not be sufficient for all desired investments, so a choice has to be made. Given the dissimilar nature of these investments, the impact of each will first have to be translated into monetary terms so that a comparison is possible. Moreover, since these investments (if realised) will have an economic impact on the organisation at different moments in the future, the value of money must be converted into a common point in time – for example the day of the decision. Let us have a look at the two competing options.

Alternative I - investing in the machine. The new machine would cost exactly 100 K Euro and result in yearly operating costs of 10 K Euro for each of the subsequent five years. After this period, the machine

²‘Rationalise’, as used here, refers to the process of justifying ones actions with plausible reasons.

would need to be replaced, but it could be sold for an estimated 5 K Euro (figure 7.2).

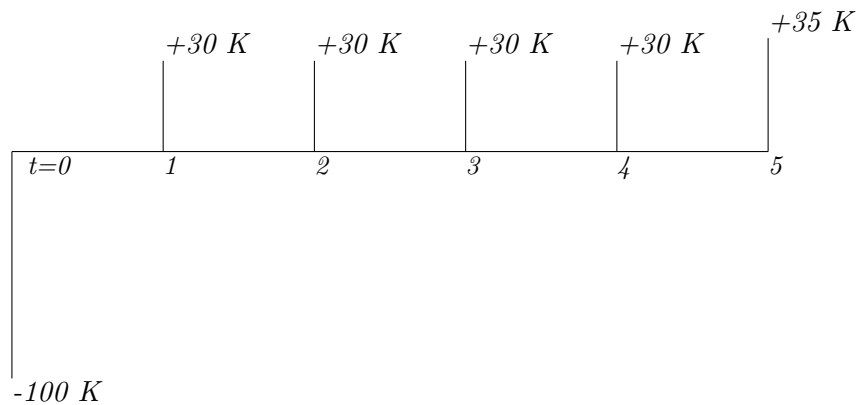


Figure 7.2: Expected payment flows resulting from investment in the microphone-manufacturing machine

The machine would produce microphones using the components put into the four containers on the side of it. Based on sales statistics from previous years, the microphones produced by this machine will generate 60 K Euro in sales each of the five years, of which roughly 20 K Euro are costs for components, marketing, etc. Thus the net payments generated by this investment during these five years following the initial investment will be 30 K Euro (60 K Euro for sales payments, less the 20 K Euro for components and various costs, less the 10 K Euro for the machine's operating costs). If the machine is sold as predicted, the final year of operation will result in an additional 5 K Euro of net payments. These flows of payments are illustrated in figure 7.2. The value of this investment alternative can be calculated as the sum of all transactions relevant to the investment – in this case:

$$(-100) + (+30) + (+30) + (+30) + (+30) + (+30) + (+35) = 85\ K\ Euro$$

However, since the payment flows take place at different moments in

time, they need to be converted into their present value, taking into account the cost of capital (interest rate). This is because the resources could have been used for some other investment which would have produced a calculated payoff or return on investment ('ROI'). Let us assume that if the organisation would not have used the money for this investment, it could have bought some stocks instead and these would yield 15% ROI per year. Therefore, this is the estimated capital cost if investing in the machine. Consequently, the present value PV of the net payments of *for example the third year* can now be calculated as (figure 7.3):

$$PV = \frac{C}{(1+r)^t} \Rightarrow PV = \frac{30}{(1+0.15)^3} \approx 20KEuro$$

Where C =capital, r =interest rate, and t =time/year

Figure 7.3: The present value (PV) of investing in this alternative

All of the net payments (including the initial cost of the machine) resulting from this investment alternative will have to be converted into their present value if we want to be able to compare this investment with the investment in information security education and training. With this conversion, we will end up with the investment's net present value ('NPV') as illustrated in figure 7.5.

As we can see in the calculations above, the net present value of the investment in the microphone manufacturing machine is 103 K Euro. This can be interpreted as "If we take into account that the alternative investment would have given us 15% interest rate, we would gain 103 K Euro if we invested in the machine".

Now it is time to compare this investment with that of investing our resources in the information security education and training programme. Converting the information security education and training investment into its NPV makes the two investments comparable – the one with the

$$NPV = C_0 + \frac{C_1}{(1+r)} + \frac{C_2}{(1+r)^2} + \dots + \frac{C_n}{(1+r)^n} \Rightarrow NPV = C_0 + \sum_{k=1}^n \frac{C_k}{(1+r)^k}$$

$$NPV = -100 + (30/1.15) + (30/1.32) + (30/1.52) + (30/1.75) + (35/2.01) = 103 \text{ K Euro}$$

Where NPV =net present value, C_0 =initial payment, C_k = other net payments, r =interest rate, and n =number of payment periods(years)

Figure 7.4: The net present value (NPV) of investing in this alternative

highest NPV is the one the resources should go into if we are to make the optimal investment decision.

Alternative II - investing in information security education and training.

The ISET programme would consist of an information security awareness project aimed at different parts of the organisation, as well as some specialised information security courses for the individuals co-ordinating the information security activities in each department. The whole ISET programme would mean an initial investment (for course material, speakers, teachers, and external courses, *etc.*) of 50 K Euro and additional yearly costs of 10 K Euro for each of the subsequent five years. After these five years, the program will be evaluated. Naturally, the information security education and training investment does not have any residual value that can be converted into funds the final year, since it cannot be sold or transferred to another organisation with ease. So far, we have identified the following flow of payments for this investment alternative (Figure 7.5).

Investment calculations usually only take into account the direct payment flows that result from the analysed investment. Therefore the investment in information security education and training does not look very good in comparison with the investment in alternative I. In fact, as

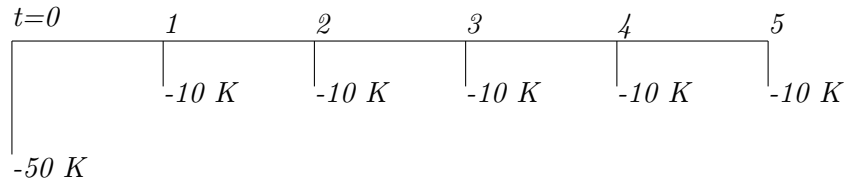


Figure 7.5: Expected payment flows resulting from investment in the information security education and training programme

observable in the calculation below, investment in the information security education and training programme will result in a negative NPV unless other payment flows than the calculated yearly costs can be identified:

$$NPV = -50 + (-10/1.15) + (-10/1.32) + (-10/1.52) + (-10/1.75) + (-10/2.01) = \underline{-83 \text{ KEuro}}$$

The investment in information security education and training is likely to have a long-term economic impact on the organisation in terms of cost reduction due to less severe and fewer information security breaches. Also, the information security education and training programme might possibly enable new business transactions to take place, as pointed out in previous sections of this paper. If organisations using this rational financial model of comparing investments are to choose the investment in an information security education and training programme instead of other investments, *indirect payments flows resulting from this decision must be taken into account*. If these indirect payments and economic effects can not be identified, it will not be possible to rationalise the investment in information security education and training.

From the example, it is evident that organisations will have to try to measure *the impact of* information security education and training if it is to be a viable investment at all. Unless organisations are given the

tools to identify the value of their education and training programme, they will not be able to justify such an investment. As a result, resources will be invested in other areas with a measurable payoff.

What can we learn from this illustrative example? This section has made explicit how organisations, according to financial investment models, generally rationalise their decisions regarding where to invest their limited resources. It has thereby clarified why organisations need to measure the broader *impact* of information security education and training. Is it evident by now that this purely financial and cash-flow perspective may severely limit the organisation's ability to make accurate and balanced investment decisions with regards to information security education and training. This leads us over to a discussion of possible information security education and training metrics and the problems associated with measuring.

7.3.4 Methods and problems of measuring

While measuring the impact of information security education and training, one is actually trying to measure the resulting change in human behaviour and its impact on the organisation's ability to reach its goal. There are several problems associated with measuring the impact if an organisational information security education and training effort, such as:

Discrepancy between what people say and what they do. The mere fact that employees, through an information security education and training programme, arrive at a measurable raised awareness of the information security regulations does not signify that they actually follow these rules or values – at least not all of them. Further, when trying to measure the impact of information security education and training, there is a possibility that some employees *do not* want to state the truth about their own level of awareness. They might be anxious concerning

what the employer's reaction would be if they admitted that they did not know of the rules they were supposed to adhere to. Therefore, from an organisational perspective, the focus should not be on what an employee knows about information security, but rather what she does with this knowledge.

Interpreting the numbers. Common sense tells us that it will be hard, or maybe even impossible, to put a number on "soft" issues, such as information security awareness (e.g. Dhillon, 1995). However, exact numbers are very seldom needed for an informed decision. Rather, some kind of grading, judgement or comparison is often needed. Another problem is that once numbers are produced, it might be hard to interpret them. What does it mean, for example, if the level of information security awareness is around 70%? Is this good or is it bad? The exact answer is: we don't know. In order to interpret numbers like these, the context has to be clear: is it a bank or is it a fast food chain? How dependent are they on their information? Quantification of "soft" issues is more useful if it can be compared with something else as a reference. For example, the level of information security awareness as measured in one financial institution might be seen in the light of the measured average level of information security awareness in all other financial institutions in that region (given that the method for measuring was the same).

What should be measured. Information security education and training is an extensive concept in itself - it embraces many facets of information security. In our view, information security awareness is manifested in the behaviour of the humans enlightened with it. This means that the action created by bright humans causes effects measurable only outside the finite domain of human knowledge or behaviour - in the technical and procedural elements of the organisation's information system. Since some or presumably large proportions of these effects are directly caused by the intellectual capital labeled 'information secu-

rity awareness', one can postulate that the estimation of these must be conducted within the formal and technical domains.

Assuming that rationalisation of investment decisions approximately follows the decision method outlined in the example in the previous section, organisations cannot be satisfied with measuring or predicting an information security education and training programmes impact on employees knowledge only. No, this raised awareness must result in a corresponding change in human behaviour. In addition, this change must result in either lowered costs or increased revenue.

7.4 Conclusions

This study has demonstrated how differing the viewpoints of the organisation and the individual are when it comes to information security education and training.

Individuals - we do not only mean computer specialists - need information security education and training to be able to minimise their security risks that they are exposed to today and will be exposed to tomorrow in the approaching information society. In addition, they want this kind of training to make them appear more valuable for the organisations. Organisations' needs are often more directly connected with their financial mission or goal. This often means that they look for information security education and training to lower costs arising from information security breaches or for enabling new business opportunities.

Organisations need to measure the effects of information security education and training because of their decision process for investments. Looking at these education and training efforts as any other investment, they demand a reasonable "return on investment" ('ROI') to rationalise the decision. If they are not provided with methods to measure the effects of, for example, a training programme, they will not be able to identify changing cost or income structures resulting from this ef-

fort. This leads to the investment in education and training looking less favourable than it really is.

From the viewpoint of individuals, assessment of these education and training efforts should ideally focus on the knowledge content. Organisations, although indirectly attracted by the knowledge, are often more interested in the behavioural changes a given course or programme can result in. This is, as we have seen, because the knowledge has to result in some change in behaviour if it is to be valuable not only for the individual, but also for the organisation. Individuals are looking for profit and so are the organisations, but their respective approaches and focuses in regard to value and assessment of education and training are sometimes incompatible.

Part III

On the Management of Information Security

This part of the thesis presents the design, analysis, and results of an empirical study into the management of information security in organisations. Data is gathered employing in-depth research interviews. Data analysis is carried out using a technique informed mainly by grounded theory (chapter 10). The main result of study - the framework of information security management - is presented in chapter 11.

Chapter 8

Introduction

8.1 Background to the research

The value of security - to individuals, to organisations, and to societies - was violently demonstrated by the September 11 terrorist attacks. In their aftermath, security as well as information security rose up on the corporate agendas - and has remained there. Information security is today considered a prioritized issue for top management and the board of directors in the vast majority of organisations. A recent global survey showed that the majority of the 1230 organisations responding even considered information security to be a CEO level priority (Ernst & Young, 2004). National surveys display similar findings; as an example, three-quarters of the 1000 respondents in a recent UK survey said that their top management or director groups viewed information security as a high priority issue (PriceWaterhouseCoopers and DTI, 2004).

Moreover, recent history has not only demonstrated the importance of information security in general, but also clearly that of information security management in particular. Corporate scandals and debacles such as the ones at Barings Bank (Lim, 1995, e.g.), Enron (Swartz and Watkins, 2003, e.g.), WorldCom (Jeter, 2003, e.g.), and Skandia (Nachemson-Ekwall and Carlsson, 2004), has presented a strong case

for the value of sound corporate governance structures (Organisation for Economic Co-operation and Development, 2004). Information security management is the key corporate governance component ensuring security for information assets. The aforementioned events have resulted in additional legal and regulatory requirements on businesses and organisations, with respect to how they manage information security. Most notably, the American Sarbanes-Oxley Act (United States, 2002) now, in effect, requires many major American companies to have efficient, documented, and certified, means of managing information security in place. Also, many thousands of European businesses are directly or indirectly affected by the Sarbanes-Oxley Act, including - but not limited to - those close to 400 European companies listed on NYSE and NASDAQ stock exchanges¹.

However, it is not only corporate scandals and resulting legislation that calls for more efficient information security management. These initiatives also come from the organisations themselves - motivated by the need to stay competitive. This need calls for proactive management of information security, rather than merely reacting to external legislative pressure or attacks. When viewing the information security efforts as a whole, organisations have found that they lack some managerial aspects of information security to really be able to reap the benefits out of their information security investment.

Thus, the value of efficient information security management to organisations is evidently widely agreed.

8.2 Research problem and contributions

Research problem

The problem addressed in this research is:

¹Including major Swedish companies such as AB Electrolux, AB Volvo, Industriförvaltnings AB Kinnevik, LM Ericsson Telephone Company, SKF AB, and Tele2 AB

*What perceptions do information security managers hold as regards the management of information security in organisations?*²

The research problem is investigated by means of in-depth research interviews with senior information security managers, followed by an analysis informed by Grounded Theory.

Contributions

Due to the exploratory nature of the research design, the research problem is answered throughout this part of the thesis. Nevertheless, answering the research problem yielded specific contributions that are described in detail in section 11. In summary, they are³:

- A diagrammatic representation of some aspects pertaining to the management of information security in organisations
- A new and improved approach to unstructured interviews
- A new research agenda for information security management

These contributions are further discussed in chapter 11.

8.3 Justification for the research

The lack of empirical research in information security management

Given the amount of attention information security has got lately - as demonstrated in section 8.1 - it is surprising that empirical research on the management of information security is lacking. The SEC 2000 conference at the IFIP World Computer Congress might serve as an

²Please refer to section 8.6 for definitions of the terms in the problem statement.

³Contributions for part II of the thesis are described in 2.4

illustration: Of the 125 papers presented at the conference, 83 % were concerned with technical aspects of information security, and only 17 % were concerned with other information security issues, such as legal, managerial, and ethical ones. Furthermore, only three (3) of the papers not concerned with technical aspects reported on any form of empirical research (Björck and Yngström, 2001).

Nevertheless, scholars and practitioners frequently prescribe strategies, ideas, practices, and standards, with regards to the management of information security and organisations. But this is most often done without studying the empirical reality in which those are to be employed.

This observation; the lack of fundamental empirical research, provides the motivation for this part of the thesis. There is a need to find out what the management of information security in organisations "is about". This is not to say that we do not have methods (standards, tools, etc.) for information security management today. On the contrary, of course we have these. Even so, what we lack is a deeper understanding of *e.g.* the actors, the threats, the objectives, or in other words - the "nuts and bolts" of information security management in organisations.

Theoretical and practical relevance of this study

This study is *theoretically relevant* because it addresses a research area which was previously largely unexplored - the empirical reality of information security management in organisations⁴. Instead of trying to apply and fit existing theories or models with this empirical field, this study attempts to build a foundation for understanding the field, by looking at it through the eyes of experienced practitioners.

This study is thus *practically relevant* because it starts to build an empirical foundation that, from a practitioner's point of view, can be used as a point of departure when creating new approaches to the management of information security in organisations.

⁴There are, however, numerous scientific studies published that look at a *part* of the empirical reality discussed here.

The aim is that this study - and other studies following a similar approach, collectively - will lay a foundation which will be valuable to practitioners and scholars aiming to create solutions and models that are based on a detailed inquiry about the field - the reality, or rather realities, which these solutions and models will eventually meet.

8.4 Methodology

As the research problem stated in 8.2 indicates, the approach chosen is based on interpreting the perceptions the interviewed information security managers have with regards to the management of information security in organisations. The objective is to arrive at views on the practical field grounded in reality and on the views formed by those who have been immersed in the practice over a prolonged time.

Given that, the ambition has been to let them present their own view, with as little influence and control from the researcher as possible. This choice calls for a research approach based on unstructured research interviews, and a data analysis based on the ideas of grounded theory, GT (Glaser and Strauss, 1967; Glaser, 1978, 1992, 1998).

While the interviews were analysed in a standard way using computer aided qualitative data analysis tools ("compatible" with GT), the interviews were conducted in a novel fashion: All interviews took as their point of departure a picture that the interviewee draw freely, showing their own world-view concerning the management of information security in organisations. The data analysis resulted in network diagrams and categories, forming the foundation for the framework of understanding presented in the concluding chapter 11. The methodology is described in detail in chapter 9.

8.5 Outline of this part of the thesis

In the next chapter (9), there is a discussion on the research method and strategy used. The reader is guided through the analysis of the empirical materials in chapter 10. The final chapter (11) in this part of the thesis presents the conclusions and their implications. A summary of the interviews, translated from Swedish to English, is also included in appendix E

8.6 Definitions

The rationale for defining key terms - and thereby establishing the definitions used in this PhD research - is that concepts often hold different semantic content among different (groups of) researchers. Where relevant, internationally recognized definitions are used.

- **Information security:** Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is characterized here as the preservation of:

- a) confidentiality: ensuring that information is accessible only to those authorized to have access;
- b) integrity: safeguarding the accuracy and completeness of information and processing methods;

c) availability: ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organisational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organisation are met. (Adopted verbatim from ISO/IEC 17799, 2000)

- **Information security management:** The management of information security in organisations. Hence, the concept denotes those activities in an organisation related to the direction and control of the security over information assets. Activities include (e.g.) assessment of threats and the current state of information security in the organisation, design and implementation of administrative (information security rules for employees, etc.) and technical (access control systems, etc.) security controls, and operation of the day-to-day efforts to preserve information security (documentation of and response to incidents, training of employees, etc.).
- **Information security manager:** An individual who has been appointed the role to be responsible for information security management (defined above) in an organisation.
- **Information security management system (ISMS):** That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources. (Adopted from BS 7799-2:2002). Hence, the concept denotes the documented and systematic efforts to preserve information security in the organisations. Compare with Quality Management Systems in line

with ISO 9000-series of standards (SIS, 1997).

- **Information security policy:** Document that states an organisation's stance on information security. It is usually less than 5 A4-pages. The policy usually includes the top management's position and high-level rules pertaining to information security. The concept is also often used to denote a more detailed document containing all the organisation's rules on information security. The intended readership of the policy is most often managers and employees within the organisation.
- **IT security:** Synonymous to "Information Security" (see definition above), albeit narrower in scope. It is concerned with the security (confidentiality, availability and integrity) of IT systems.
- **Perception:** A mental image (Merriam-Webster, 2004), impression, and understanding of a phenomenon or artifact (e.g., information security management) formed by the process of observing (perceiving).
- **Risk assessment:** Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence. (Adopted from ISO/IEC 17799, 2000)
- **Risk management:** Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost. (Adopted from ISO/IEC 17799, 2000)

8.7 Delimitations of scope and key assumptions

The problem statement in section 8.2 already indicates the most important delimitations of this study. Here is a more detailed exposition of the delimitations:

Perceptions - not physical reality

Firstly, the unit-of-analysis is *perceptions*. Thus, the study is not concerned with exactly how information security is managed in one (or many) organisations. Instead, the study is concerned with the interviewees' perceptions, formed by the process of perceiving the events of - and being immersed in - the management of information security in many organisations during many years of practice.

Managers and consultants - not users

All interviewees are interviewed as experts in their field. They have been working for different organisations trying to solve the problems of information security. An alternative approach would have been to interview users or other employees - *e.g.* those who are subject to the controls often created by the managers and consultants. Nevertheless, since the focus of this study is to learn more about the reality that the managers of information security meet, in order to be able to better cater for their needs in terms of methods, tools, etc. in the future, it is natural to start asking them. It is also possible to assume that they (the experts) have a more holistic view of the information security problem in those organisations than the average users.⁵

Individual Swedish cases

These were the two delimitations that were indicated by the problem statement. However, there are also two additional delimitations that would be mentioned to put a boundary around this study.

Firstly; all interviewees were from Sweden. The assumption is that even though they were all from Sweden, the results from the study will be of interest also for readers in other countries - especially other countries

⁵Having said this, it would be another interesting study to interview users and ordinary employees to try to elicit their views on information security in their workplace.

in the European Union which share a similar culture and use similar approaches to managing information security. Nevertheless, there are no claims made that any given manager of information security in *e.g.* Denmark will have the same or a similar world-view as the interviewed ones. That leads us over to another important delimitation.

Secondly: this study is concerned with describing and interpreting individual cases rather than trying to formulate laws. In other words, it is ideographic⁶. rather than nomothetic⁷. Hence, this is not a survey of how information security is managed in organisations in Sweden, in Europe, or in the World. Instead, this study aims to build the foundation for a more thorough understanding of the subject at hand by seeing it from the eyes of a few experts.

These delimitations set the boundaries for the conclusions of this study, even though its implications are more far-reaching.

8.8 Chapter summary

This chapter laid the foundation for this part of the thesis by stating the research problem, justifying the research by discussing its theoretical and practical relevance. Further, it defined the central concepts used and gave an overview of the methodology. An outline of the coming chapters was given, followed by a discussion on the delimitations within which this study takes place.

⁶Concerned with individual matters of fact

⁷Concerned to formulate general law

Chapter 9

Methodology

9.1 Overview of Grounded Theory

Grounded Theory (hereafter referred to as "GT"), created by Glaser and Strauss (1967) is a research approach which describes steps to be taken; from the start with a broad research question, via data gathering and analysis, to arrive at a theory or model grounded in the reality studied. By following GT, one will end up with a theory or model that fits the data gathered, and can explain the data.

GT is based on the assumption that often the most fruitful theories are built up from the empirical world into theoretical abstractions, rather than the other way around. An alternative approach to GT would be to take an existing theory in a similar field as the one studied here, and then try to apply that theory to the empirical setting studied. This would then be a more traditional hypothetico-deductive study, which is very common in doctoral research. The reason that a GT-based approach was chosen before a more traditional approach is that the objective this time was to arrive at a model grounded in the empirical field, with the aim of creating a foundation for practitioners and scholars to better understand (influence, control and predict) information security management.

The main drawback of GT is that theories and models created using

this approach tend to be very close to the data, which means that the abstraction level might suffer. They run a risk of being overly specific, and thus might fail to help us understand other situations.

9.2 The principles of Grounded Theory

As implied above, GT is an approach which consists of a set of tools and principles. These are concerned with research design, data gathering, data analysis, and theory construction:

Research design. GT requires the researcher to start with an "open mind". In this way, it does not support hypothesis testing. Even if the research area is set, the actual formulation of the research question, and the focus of the research, is allowed to change during the period of the study.

Data sampling. GT does not depend on statistical sampling of a number of subjects from a larger population. This is due to the nature of knowledge that is created using GT: Knowledge emanating from a GT process will not say "how things are" in the world (or in a larger population), "how many" or "how much". Instead a GT approach acknowledges that a large part of our reality is continually created and re-created by individuals living and perceiving their world. Therefore, there is a degree of subjectivity that has to be acknowledged rather than suppressed. From this viewpoint, statistical sampling becomes less interesting and fruitful - instead GT offers the notion of "theoretical sampling". Theoretical sampling means that sampling is not necessarily done before the data is gathered - it can be done during the course of the study. For example, the answer of one respondent could direct the researchers to another source that could help to further shed light on the phenomena studies.

Data analysis. GT allows that all the empirical material, such as interviews and pictures, are recorded for later analysis (although this is not a methodological requirement). The most common materials in GT studies are interviews, and the common approach is to type all interviews out as text verbatim. The data analysis is then done on the actual text by reading each sentence and asking questions such as "what does my data say", "what category indicated this event", and "what is happening in the data?" (Glaser, 1978; Starrin et al., 1997). Each sentence is then coded by a category that indicates the content of that sentence. A sentence can have more than one code, because it can mean different things. This first coding process is called open coding (Glaser, 1978). GT allows the researcher to go over to selective coding, which means to code for one specific category, when it is clear that this one category is at the core for the research problem at hand.

Theory construction. When all coding of data is done, theoretical coding commences. This means to relate the codes to each other as to form a model of how they fit together. This then forms the basis of the emerging theory or model. Hence, theories created using a GT-based approach are based on concepts (codes) related to each other.

9.3 Research method of this study

There are almost as many GT interpretations as there are researchers who have attempted studies based on GT. Although one should always strive towards using the method as the originators intended, this can be a challenge as noted by *e.g.* Gustavsson (1998, 125) and Starrin et al. (1997, 46). Even the two originators of GT had a long ongoing debate of what they actually meant GT to be when they together created it almost 30 years ago. This is evident in the dialectical tension between the two books written by Strauss and Corbin (1990) and Glaser

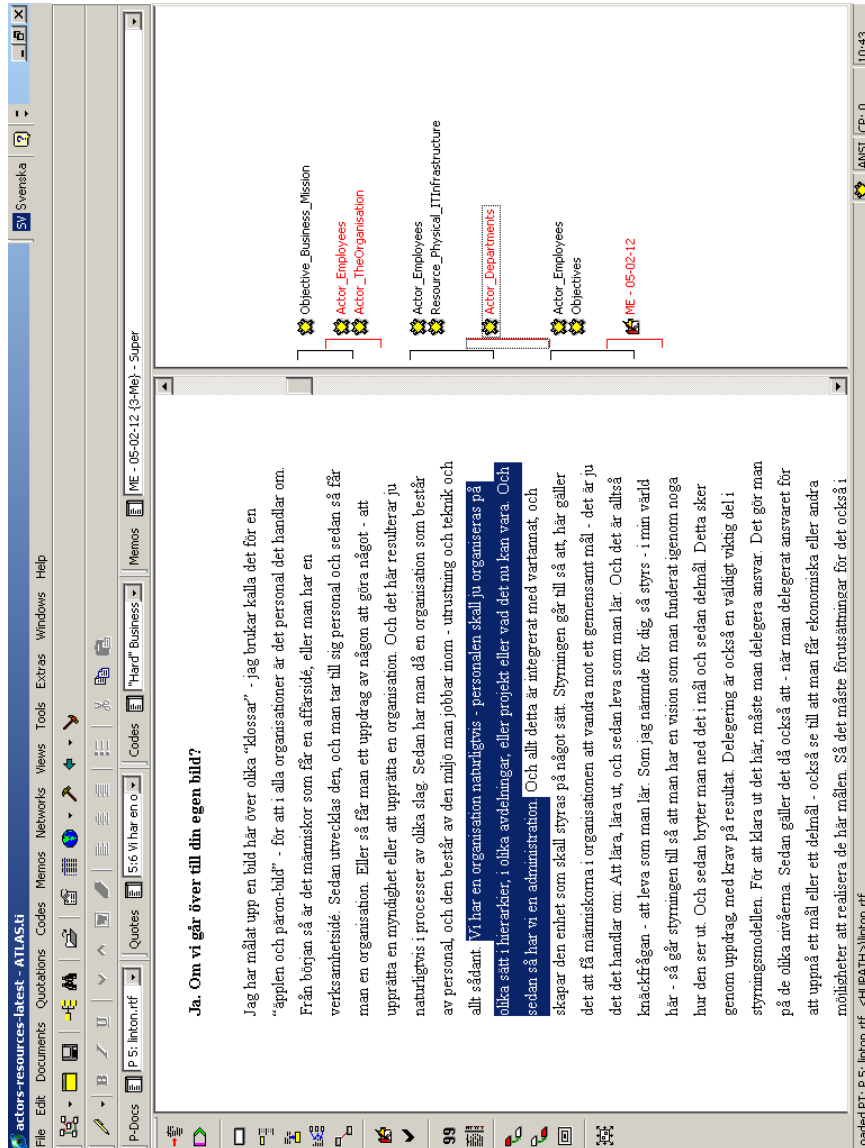


Figure 9.1: The main user interface in Atlas.ti.

(1992), respectively. This debate resulted in two "flavours" of GT - the "Glaserian" and the "Straussarian" ones. GT in this study is yet another interpretation, especially tailored to the problem at hand, while trying to preserve the originators' intentions:

Research design. The research question was kept open throughout the study. There were no hidden hypotheses underlying the study. The empirical material was collected via in-depth unstructured interviews with experts in the field. These were recoded and transcribed word-by-word. The interviews did not have pre-determined questions in order not to disturb the interviewees' own views. Instead the interviews were focused around a picture that each interviewee drew before coming to the interview. This approach can be viewed as an operationalisation of what Gustavsson (1998, 52) refers to as the "circular approach", meaning that the researcher should avoid asking *too* direct questions if possible. Each interview started with a discussion on the respondents' personal background in the area, and then moved to their picture that described their "world-view" on the management of information security. They explained their picture, and the interview went on exploring this picture in depth. Thus the researcher and the respondents "circled" in on the subject with the respondents' own picture as the point of departure. Each interview lasted circa one hour.

Data sampling. For several reasons the approach that was chosen did not include "theoretical sampling" offered by GT. Instead, the interviewees were selected as being experts in the field. They were all senior managers and consultants in the area of information security management and that is why they were asked to participate in the study. Eight potential interviewees were asked by formal letter if they wished to participate; all eight accepted.

Data analysis. As described above, the interviews were transcribed - in total close to 200 pages of text. Then the texts were fed into a

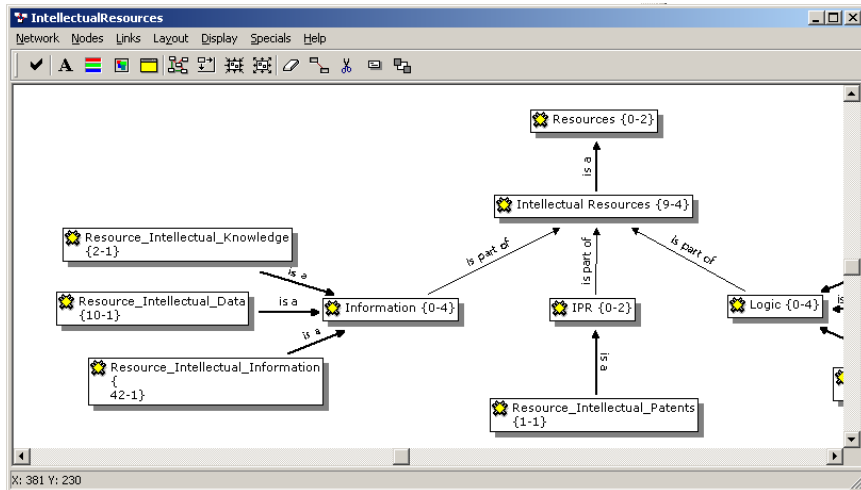


Figure 9.2: The network editor in Atlas.ti.

software-based tool for qualitative data analysis that supports the principles of GT, called atlas.ti (Muhr, 2004). The tool does not do the actual analysis, but it helps the researcher to keep track of hundreds of codes, categories, quotations, and theoretical notes (see picture 9.1)

Theory construction. The theoretical coding was aided using the network view of the software tool. Some codes were merged, new super-codes keeping lower-level codes together were created, relations between codes were set (see figure 9.2).

9.4 Personal background and influence on the research process

My personal background does influence the research process in several ways. I will first explain in what ways my professional experience influenced the choice of research question, and shortly discuss the conse-

quences of this fact. Then I will present how my educational background has affected the general perspective assumed in this work.

Professional experience

I embarked on this research endeavour out of personal interest. I was exposed to many different organisations as an IT auditor and information security consultant at one of the world's leading professional services firm. My responsibility as an auditor was to assess the degree of control these organisations had over their information resources, as a part of the annual external financial audit. As a consultant, I helped other organisations to establish this kind of control via technical, administrative, and other measures. All in all, my experience from these assignments left me with a question I really wanted to settle: Why is it those organisations' information resources very often are left vulnerable, despite the fact that the same organisations clearly attempt to manage information security? My feeling was that reflection over this and related questions was needed if we (information security professionals) were to be able to really help organisations with their information security efforts. Consequently, when the opportunity materialised, I decided to devote the time needed to really explore the different facets of this question. Even though the exact research question, method, and perspective have evolved over time, this personal experience of mine has been and continues to be the main motivating force in this work. In other words, the broad research question is clearly affected by my personal background:

In deciding to explore this research question, I also chose not to explore other alternative questions. It is possible, or even probable, that I would have tackled a different question if my personal background would have been different.

Now, having explained in what way my personal background and experience in the area of information security affected my choice of research question, it is also important to note some factors that did not affect this choice. This research project is not a part of any pre-defined

research programme - I have been free to decide on everything (after discussing with my advisor). This research project is not externally financed by any industry or other party. It is financed directly by the Swedish Government via the university system. Hence, there are no external pressures on what the research should be focusing on, what ideal results should be like, or what the most suitable research method would be. There are no hidden agendas or secret stakeholders.

Educational background

My first degree is in business studies and economics. I pursued two foci during these early years of university education: management and control. After this, I went on to the London School of Economics (LSE) to focus on information systems security, and was awarded a masters degree there. LSE is really a business school, so it might seem odd that they offered a masters in IS security. But for me, it was a perfect match. The security scholars at the LSE have their particular view on information security which can be summarized by the statement: "the information security problem is about people, not primarily about technology". This view was successfully transferred to me, and I am heavily affected by the teachings at LSE today. Hence, it was only natural for me to focus on the management problem rather than the technology problem in information security.

Chapter 10

Analysis of Data

10.1 Introduction

The preceding chapter presented the methodology used for data gathering and analysis. The aim of this chapter is to present the results of applying that methodology.

The results presented here are based on 637 quotations that were marked in the transcribed interviews. These quotations were categorised into 184 categories and resulted in a total of approximately one thousand codings.

Since the interviews were conducted in Swedish, no quotations are used here, as otherwise common. To enhance the transparency of the data analysis process, a complete log which shows each step from quotations, via codes, into these models, is available upon request. Furthermore, a summary of each interview, translated into English, can be found as an appendix (E) to the thesis. The motivation for including these summaries is so that the reader can gain personal insight into the content of the interviews, *albeit* on a high level.

The analysis focuses on the objectives, actors, resources, threats, and controls which appeared in the empirical material. This focus was however not pre-determined, but emerged from the data.

10.2 Analysis of objectives

Security Objectives

Objectives can be divided into two main categories; business objectives and objectives relating to information security - security objectives. Starting with the security objectives, the ones that quickly emerged in the material were objectives related to properties of information. They were:

Security Objectives relating to properties of information

- Availability
- Confidentiality
- Integrity

These are also the most common objectives in mainstream literature on information security. In addition to these, properties such as accuracy, reliability, and relevance of information were discussed, but the interviewee who mentioned these identified them as falling outside the scope of information security as traditionally defined.

However, the interviewees also discussed many other security objectives, not pertaining to the property of information assets. Most notably those pertaining to users or employees and those related to the communication of information. They were:

Security Objectives pertaining to employees

- Awareness
- Privacy

Security Objectives pertaining to communication

- Traceability

- Accountability

Awareness refers to employees being aware of the importance of information security, and the top management intentions thereof, so that they can act in a manner that preserves security.

Privacy deals with the individual's right to be left alone, and applies to employees as well as customers.

Traceability means that it should ideally be possible to trace any event in the information (technology) system to a specific individual (actor) or automatic process.

Accountability is related to traceability. It denotes the principle that it should be possible to hold individuals responsible for the actions that they take in an information system.

Business Objectives

Although the interviews were about the management of information security and not about business management in general, a number of business objectives emerged in the material. They are divided into "hard" and "soft" types of objectives, where the former implies traditional types of objectives that are often easier to measure objectively, and the latter refers to those business objectives that are more difficult to measure, but still have a bearing on an organisation's ability to survive. The properties or values of these "soft" objectives are very much dependent on the perception of stakeholders, such as customers, owners, etc.

"Hard" Business Objectives

- Financial
- Efficiency

"Financial" and "Efficiency" here are not really objectives, but rather categories of objectives that were further specified in the empirical material. For example, some financial objectives that were mentioned

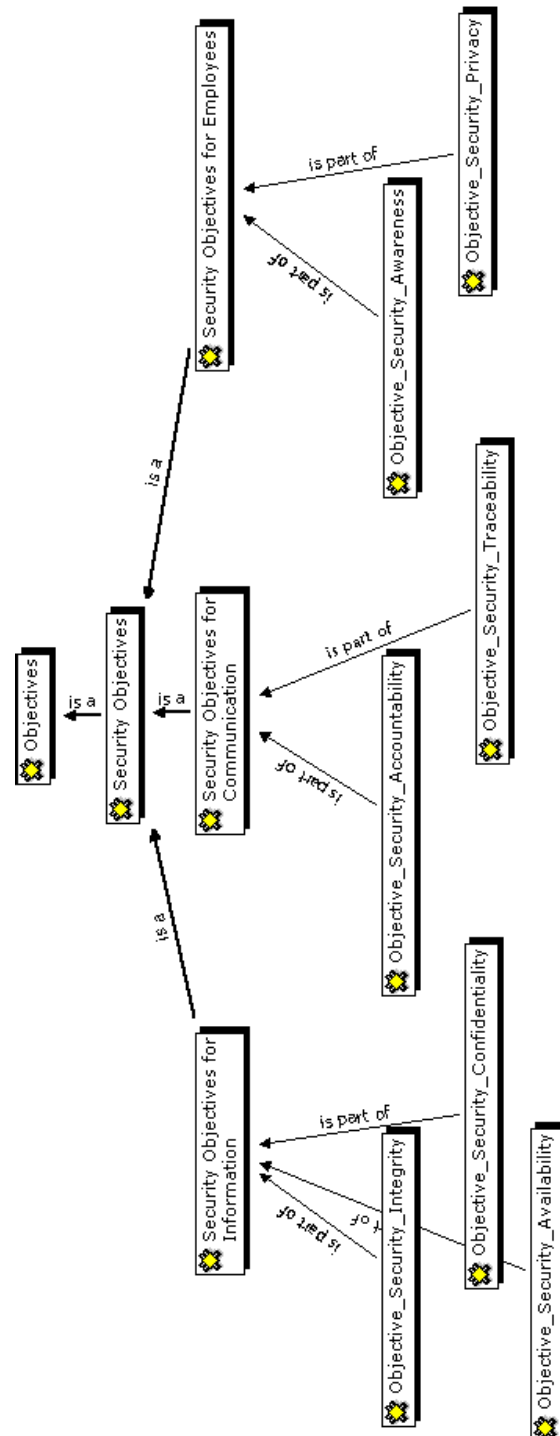


Figure 10.1: Focused network view: Security Objectives

were "profitability", "shareholder value", "return on capital employed", "price to earnings", etc. Some efficiency-related objectives were efficiency relating to human resources, efficiency relating to the use of IT in the organisation, etc.

"Soft" Business Objectives

- Quality
- Trust

"Quality" and "Trust" are more difficult to measure, but are still very central to the problem under study. Several interviewees mentioned security as being a part of quality, or at least affecting quality in a profound way. The business objective "Trust" has to do with how outside stakeholders view the organisation. For example, an organisation's "good-will" would be part of this concept.

10.3 Analysis of actors

Actors are here active subjects like individuals, groups, and organisations affecting or being affected by the management of information security, as seen from the viewpoint of an organisation. These actors can be divided into two main categories: those that are external to and those that are internal to the organisation (see figure 10.3).

The external actors that emerged from the interviews fell into five distinct categories: delivering, monitoring, opinion, competing, and buying actors respectively.

External actors

Delivering actors Business Partners, Security Solutions Vendors, Insurance Companies, IT Outsourcing Partners

Monitoring actors Auditors, IT auditors

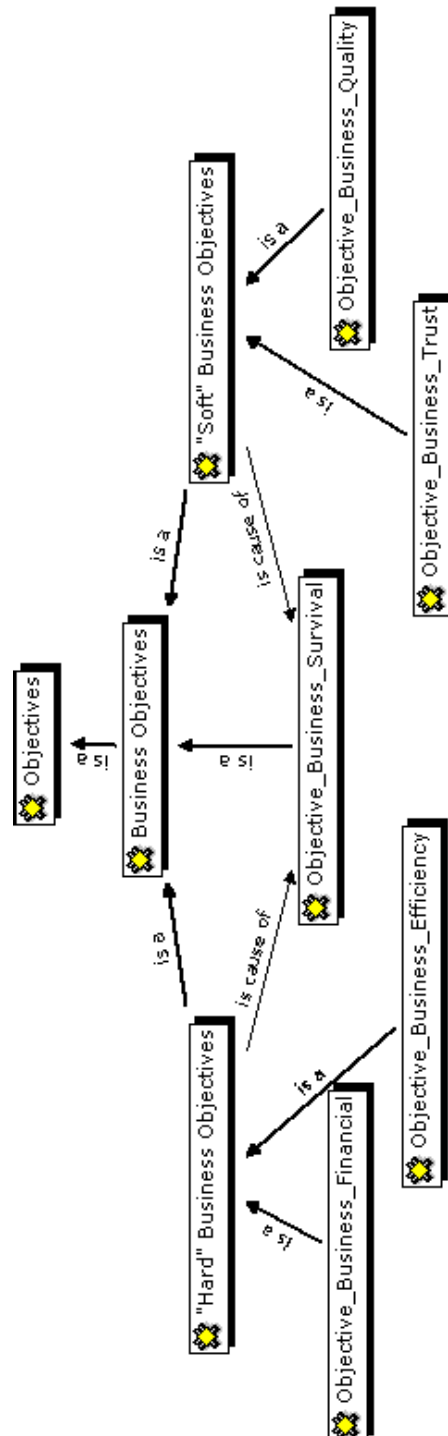


Figure 10.2: Focused network view: Business Objectives

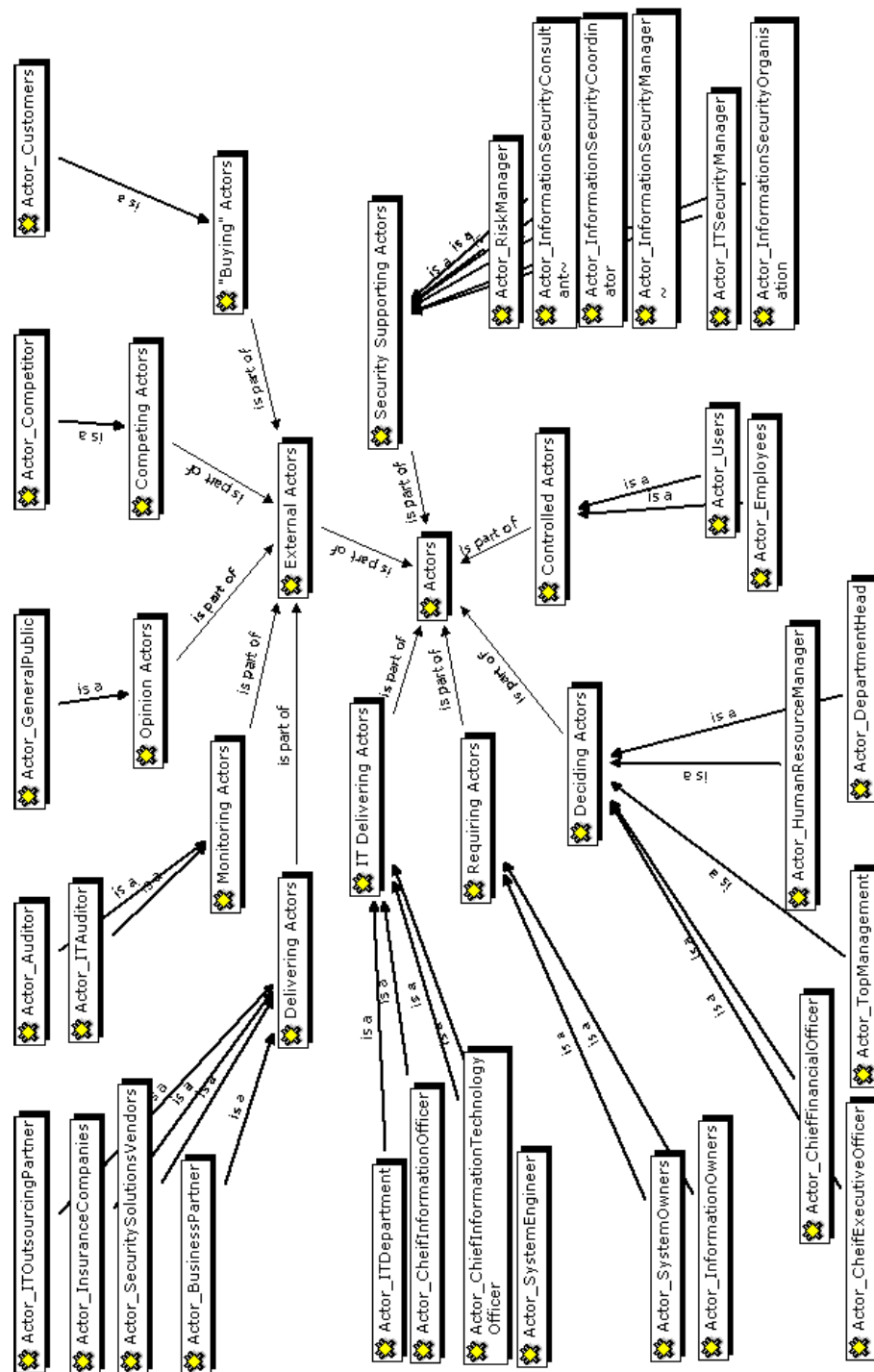


Figure 10.3: Focused network view: Actors

Opinion actors The General public

Competing actors Competitors

”Buying” actors Customers

This resembles a systems view of the organisation. One can discern *e.g.* the inputs (delivering actors), the cybernetic control system (monitoring actors), and the receiver of the outputs (buying actors). The competing and opinion actors can be seen as the organisation’s systemic environment.

Moving into the organisation itself, the different categories of actors were, based on their role: IT delivering, Requiring, Deciding, Controlled, and Security supporting actors.

Internal actors

IT Delivering actors IT department, Chief Information Officer, Chief IT Officer, System Engineers

Requiring actors System Owners, Information Owners

Deciding actors Top management, Chief Executive Officer, Chief Financial Officer, Human Resource Manager, Department heads

Controlled actors Users, Employees

Security supporting actors Risk manager, Information security consultant, Information security coordinator, Information security manager, IT security manager, Information security organisation

The internal actors have specific tasks in relation to the management of information security. The IT department, populated by the systems engineers, and led by the CIO or CITO, delivers the IT solutions (IT delivering actors, supply-side). The information and systems owners (requiring actors, demand-side) make requirements on both information

technology need in general, and also on the security they need. The level of security ordered is then ideally delivered by the security supporting actors; the consultants, coordinators, and managers of information security. Technical and administrative controls (countermeasures, safeguards) are put in place to control (and motivate) users and employees (controlled actors). The final decisions and the strategic apex of information security is comprised of the deciding actors, including top management and department heads, including *e.g.* CEO, CFO, HR managers.

10.4 Analysis of resources

Resources are in this context such things that are to be protected with the collective information security management effort. Resources have a value for the organisation in pursuing its business activities and are a part of the information system (in the broad sense) of the organisation. They fall into two broad categories - physical and intellectual resources.

Physical resources

Physical resources can further be divided into those relating to communication, computing, and facilities.

Physical resources pertaining to communication

- Telephones
- Modems
- Local Area Networks
- Private Branch Exchanges

Physical resources pertaining to computing

- Personal Computers

- Handheld Computers
- Laptop Computers
- Terminals
- Storage Media
- IT Infrastructure

Physical resources that are part of facilities

- Physical resources
- IT Hall
- Office Building
- Production facilities
- Furniture
- Cables

All these physical resources are of very different character (a building, a cable). Nevertheless, they are all supposed to be protected by the collective information security management efforts.

Intellectual resources

Intellectual resources can further be divided into information, IPR, and software.

Intellectual resources that are made up of information

- Data
- Information
- Knowledge

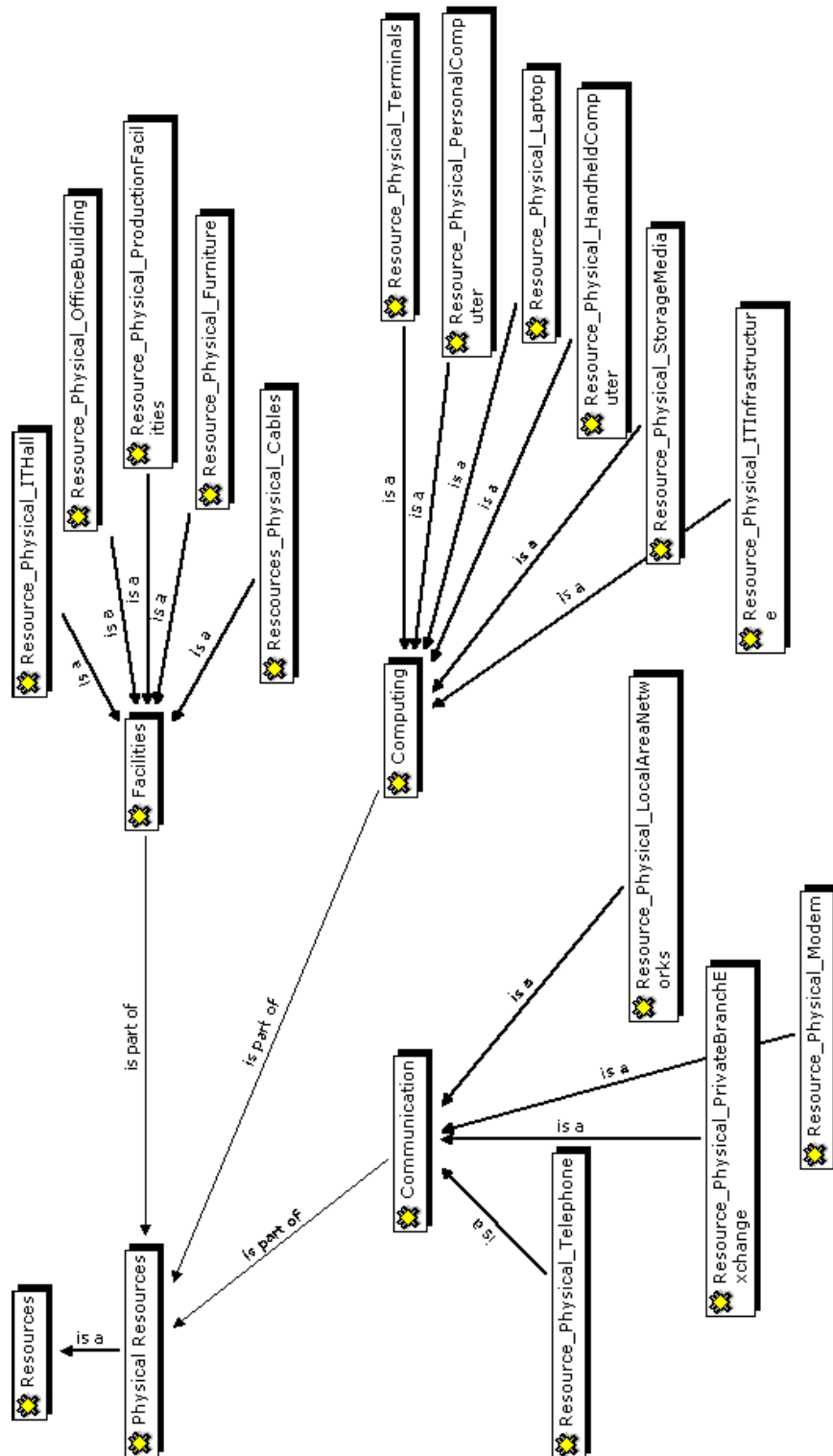


Figure 10.4: Focused network view: Physical Resources

This follows the classic triad of data, information, and knowledge. This is at the heart of what information security management is aiming to protect. Data can be seen as the raw material in computer systems or information that is yet to be interpreted by a human; information is data with an interpretation, and knowledge can be seen as information that is ready to be applied.

Intellectual resources that are IPRs

- Patents

Intellectual property rights (IPRs) are generally trademarks (e.g. brand names), copyrighted works (e.g. books, movies, developed software), and patents. However, only patents came up in the empirical material. IPRs are one distinct category of intellectual resources that information security can help protect. IPRs are called IPRs because they are already to a certain extent protected by the law.

Intellectual resources that are software

- Application Systems
- Web Systems
- Operating Systems

Software resources have a special character in that the protection they need is often to preserve the integrity of the code, so that the execution of the code will not result in unwanted modification, destruction, or disclosure of the organisation's data, information, or knowledge. Thus it is not the applications, the web, or the operating systems themselves that are worth protecting: the focus is rather on trying to protect other information assets from them.

10.5 Analysis of threats

Under this heading, everything that has to do with the threat information security management is trying to protect against is analysed.

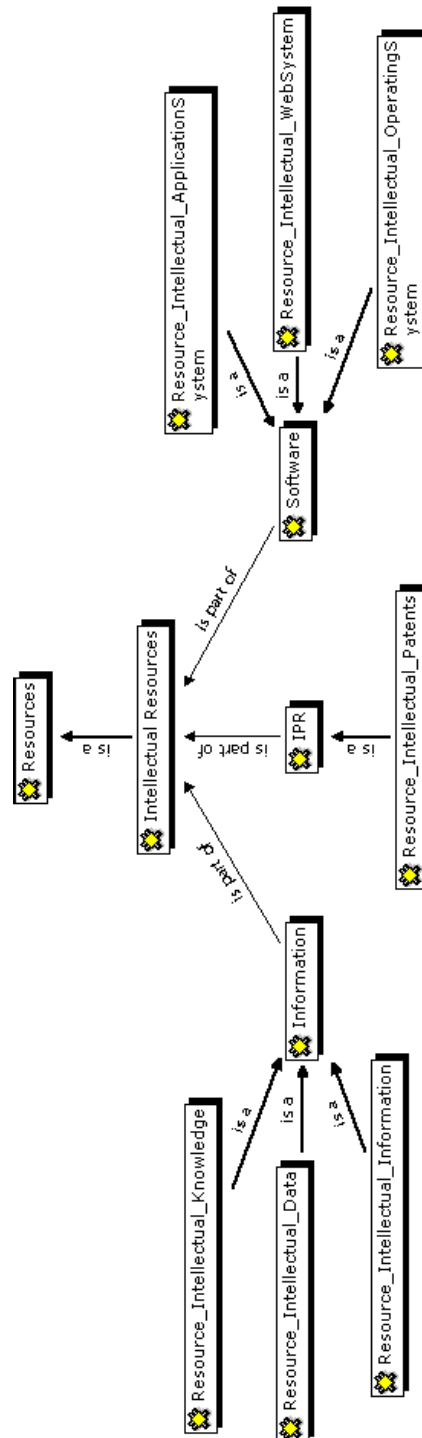


Figure 10.5: Focused network view: Intellectual Resources

This includes categories of unwanted scenarios that, if they materialised, would affect security negatively, categories of wrongdoers, and the consequences of security breaches.

Threat agents

Threat agents, as they appeared in the material, can be divided into insiders and outsiders. Interestingly, very little was actually said in the interviews about threat agents. Nevertheless, employees were mentioned frequently as a potential source for both mistakes and deliberate acts resulting in security being compromised. Note that employees and users are also listed as benevolent actors in the preceding analysis. The other category of threat agents is outsiders - most often seen as the hacker.

Threat agents

- Insiders
- Outsiders

Threat scenarios

Threat scenarios that emerged in the material ranged from very detailed to more broad ones - from attacks via e-mail (mailbombing) to terrorism.

Threat scenarios

- Hacking
- Computer virus
- Break-in
- Fire
- Mailbombing

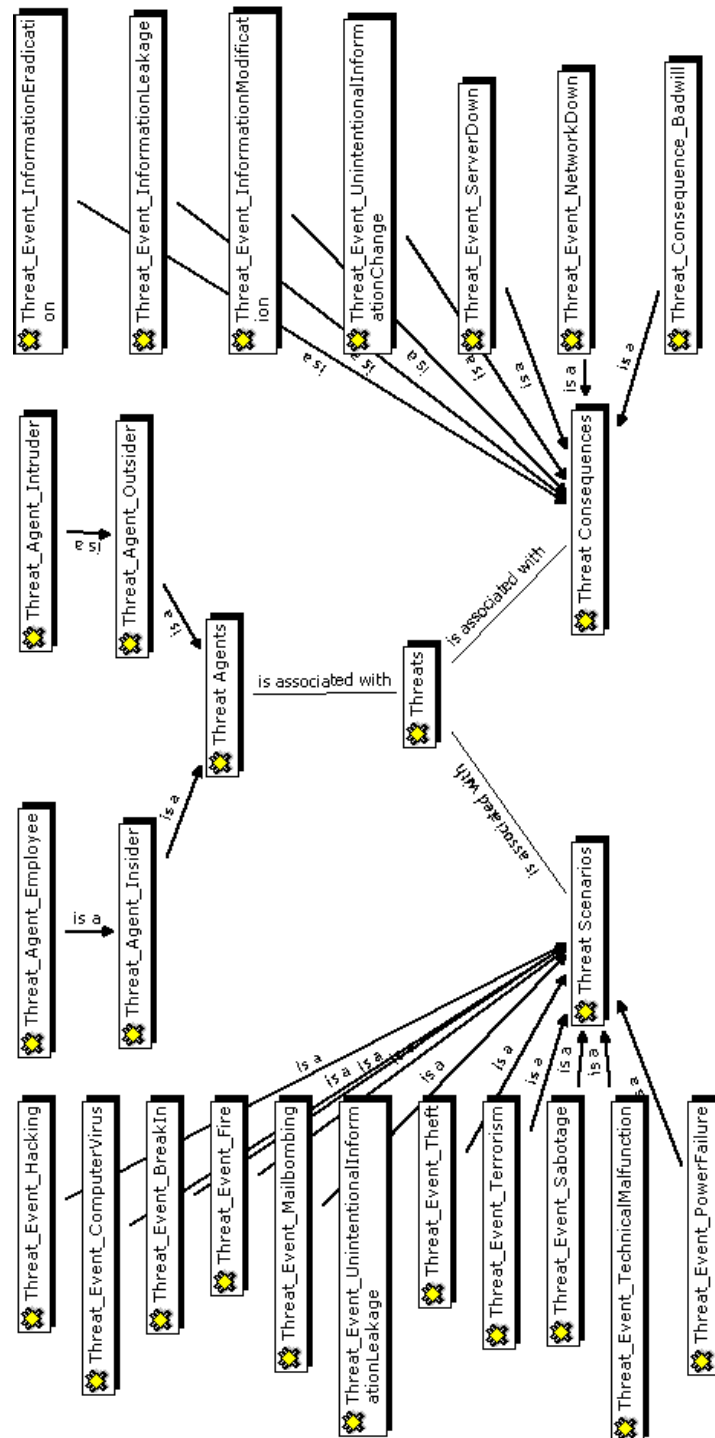


Figure 10.6: Focused network view: Threats

- Unintentional information leakage
- Theft
- Terrorism
- Sabotage
- Technical malfunction
- Power failure

These threat scenarios could further have been divided into unintentional (unintentional information leakage), deliberate acts (hacking, break-in, mailbombing, computer virus, theft, terrorism, and sabotage), and "acts of God" (power failure, technical malfunction, fire).

Threat consequences

Threat consequences

- Bad-will
- Information Eradication
- Information Leakage
- Information Modification
- Network Down
- Server Down
- Unintentional Information Change
- Technical malfunction
- Power failure

Threat consequences are important to consider when conducting risk analysis for information security. They answer the question "What will happen if threat scenario X materialises?" Some of the consequences are more direct (like a server that "goes down") and others are of more indirect character (like the bad-will that follows after a security breach is reported in the media).

10.6 Analysis of controls

Controls are all those countermeasures or safeguards that are put in place in an organisation and that make up the information security management system. Example of controls can be rules in the information security policy, a packet-filtering firewall, or a physical door with a lock. Controls of three types emerged from the empirical material; these were administrative, technical and physical controls.

Administrative controls

Administrative controls are those that try to affect the formal (e.g. by stating rules in a security policy) and informal parts (e.g. by increasing employee awareness by education and training) of information security.

Administrative controls

- Business Continuity Plan
- Education
- Incident Handling
- Information Classification
- Information Security Management System
- Information Security Policy
- Security Goals

- Standards
- Security Strategy

Technical controls

Technical controls are those that are installed and operated in the computer systems. Some administrative controls, like rules, can also be matched by technical controls that e.g. enforce the rules.

Technical controls

- Access Control
- Antivirus
- Automatic Patch Updates
- Backup
- Biometrics
- Encryption
- Firewall
- Intrusion Detection

Physical controls

Physical controls are those that try to protect the organisation's information security by physical means. For example, a guarded reception in an office building would be an example of a physical control aiming to keep the organisation's physical security perimeter intact.

Physical controls

- Access Control
- Alarm System
- Fire Protection

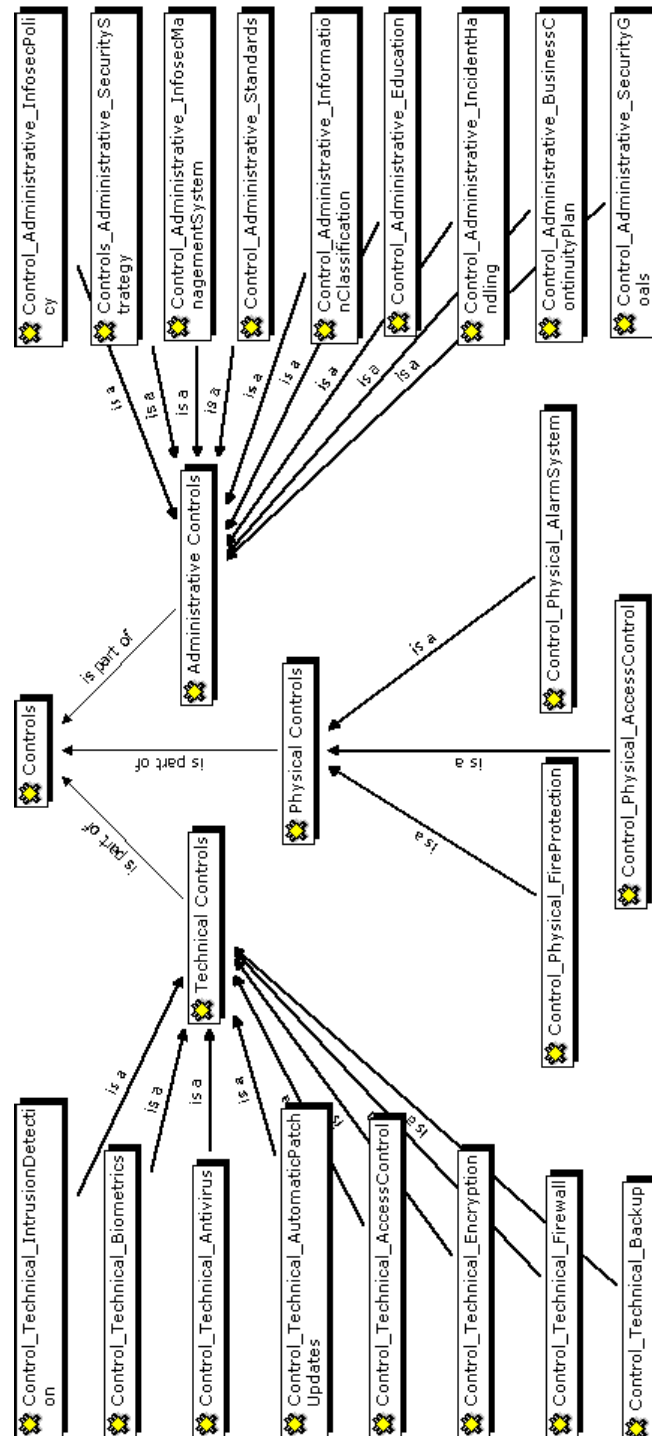


Figure 10.7: Focused network view: Controls

10.7 Chapter summary

This chapter presented the results of the data analysis in the form of diagrammatic representations of different aspects of the management of information security in organisations. These aspects were: objectives, actors, resources, threats, and controls.

Chapter 11

Conclusions and implications

11.1 Conclusions about the research problem

The research problem stated in section 8.2 was "*What perceptions do information security managers hold as regards the management of information security in organisations?*". This study approached the problem from an empirical point of view and without using a pre-defined theoretical framework or perspective. Instead, a data-gathering approach based on unstructured in-depth research interviews with experts was employed, and the subsequent data analysis was done in line with the principles of Grounded Theory.

The results, presented in summary below and throughout chapter 10, indicate how the interviewed experts perceive information security management. Focus throughout the study has been to arrive at an integrated view based on their perceptions rather than trying to emphasize the differences between them.

Owing to the nature of the research problem and the research design, the research question can not be answered in a single sentence, nor can all the conclusions be spelled out in this single concluding section. The

Objectives	Business	Soft		Hard								
	Security	Info	Empl	Comm								
Actors	Internal	i1	i2	i3	i4	i5						
	External	e1	e2	e3	e4	e5						
Resources	Intellectual	Info	IPR		Software							
	Physical	Communica	Computing		Fascilities							
Threats	Scenarios	s1	s2	s3	s4	s5	s6	s7	s8	s9	10	11
	Consequences	c1	c2	c3	c4	c5	c6	c7				
	Agents	Insiders					Outsiders					
Controls	Administrative	a1	a2	a3	a4	a5	a6	a7	a8	a9		
	Technical	t1	t2	t3	t4	t5	t6	t7	t8			
	Physical	Access control			Alarm system			Fire protection				

Figure 11.1: An integrated view of the results

answer to the research question is nevertheless summarised in the figure 11.1 so as to give an overview of the areas in which the results are situated. Please refer to chapter 10 for more details on the different parts illustrated in the figure here. The next two sections will focus on what these results mean for theory and practice.

11.2 Implications for theory

11.2.1 Knowledge characterization

This study aimed at an ideographic description of the interviewees' perceptions. It follows that it was not an attempt to arrive at universal laws or the causes and effects of information security management in general.

The knowledge created is true and correct in the sense that the results, illustrated by the model depicted above, are based on the experts' views. Care has been taken, throughout the application of the new interview technique based on the interviewees' own illustrations, not to distort these views by asking pre-defined questions. Furthermore, the data analysis process has been made transparent, so that one can go back and study in which way each quotation from the transcribed interviews backs up the models through a web of almost one thousand relations (codes). In this way, it is safe to say that the model presented does in fact say something about the experts' perceptions and. What the model and this study do not reveal is whether these perceptions are indeed mirrored in the thoughts of the larger population of information security managers in Sweden, Europe, and on a global scale.

Thus, the aim has not been statistical generalisation to an underlying larger population, but rather analytical generalisation; moving from the empirical material up into codes and supercodes, to make sense of the material. Through this analytical generalisation, the results become both less dependent on the context and more applicable in other situa-

tions. Nevertheless, the boundaries of the applicability of these results will be tested by the readership of this study and the users of these results.

11.2.2 Contributions to the body of knowledge

The results of this study - the different elements and their properties illustrated in the figure 11.1 - can be described as the basic building blocks of information security management. In order to arrive at a solid foundation for a more systematic global research programme in information security management, we need to start building from the empirical reality in which this applied area is actually situated. Noting the lack of systematic empirical research on information security management in general, this study starts this work by eliciting the basic building blocks of a more complete theory or model of information security management. Once we have the basic structures of information security management laid out, we can start studying the different parts more systematically, and compare results throughout the academic world.

Although this study alone can not achieve a complete "theory of information security management", it has contributed by starting to map out the empirical terrain of the field.

As a secondary contribution, there is the new method created in this study for the unstructured interview. The problem was not to affect the interviewed experts by asking pre-defined questions. We wanted to let them speak from their own points of view, to arrive at their perception of the area. The solution was to create a novel method used before and during the interviews: Each interviewee was sent an empty sheet of paper with instructions to draw their own perception with regards to information security management. Then each interviewee brought this to the interview, and the whole interview focused around their own illustration. No pre-defined questions were used. This method proved to be efficient, and could be used by other scholars in the field.

11.3 Implications for practice

Practitioners - *e.g.* information security managers, consultants and IT auditors - need methods and tools for information security management that help them maintain a cost-efficient level of information security. These methods should ideally be based on the empirical reality in which the practitioners are situated. By studying that reality, and by describing different dimensions of its objectives, actors, resources, threats, and controls, this study creates a map of this organisational terrain. It works like a blueprint for information security management. Practitioner can compare their own reality with the blueprint and identify important aspects that may be lacking or that have been forgotten in their own organisation.

Consultants and standardisation bodies can use the results to create new methods that are based on the research findings, so that new - empirically based - tools can become available to practitioners.

11.4 Further research

11.4.1 Study of assumptions on information security management

The focus in this study was to elicit experts' perceptions of rather concrete elements of information security management. An alternative approach could have been to focus on how each interviewed expert perceives information security management on a more abstract level. This would reveal if there are differences in the set of assumptions held by the experts in relation to the "world" in which their work takes place. Such an approach would identify differences in perceptions, rather than attempt to arrive at an integrated view of these.

During the data analysis phase, these differences sometimes lit up in the empirical material. However, they were not easily captured and described while applying the data analysis techniques of Grounded The-

ory. This is due to the nature of the method, which is somewhat geared towards 1) analysis on a low abstraction level; and 2) finding similarities (creating integrated views) rather than identifying differences.

As individuals we have different sets of assumptions about phenomena and artefacts in our environments - so also with these experts. These assumptions affect the choices we make. Thus, an information security manager or consultant holding one set of assumptions will probably make other choices when managing information security than one holding another set of assumptions (all else being equal). This thought is in line with McGregor's "Theory X" and "Theory Y" (McGregor, 1960) which was concerned with how managers' assumptions of their subordinates (lazy or seeking responsibility) affected work efficiency.

Although no systematic analysis was made concerning possible sets of assumptions, a few interesting dimensions appeared during this study. These dimensions were:

Nature of the threat Is the threat to information security mainly mistakes or deliberate acts? Is the source of the threat mainly internal or external to the organisation?

View on employees Should employees be trusted, or do they have to be controlled? In relation to information security; should they better be coerced or motivated to follow rules?

Predictability of the future Is it possible to predict the future with regards to information security for the organisation, so that one can optimize the level of investment in security, using risk analysis methods? Or is the future not predictable at all?

If there are indeed different types of information security managers with different sets of assumptions and thus different answers to the questions above, this would undoubtedly affect how they choose to manage information security in their organisation.

To sum up: an alternative approach could have been to identify those different sets of assumptions, study what kind of management those assumptions lead to, and finally to study if and under what circumstances one of the resulting management approaches is more efficient than another.

11.4.2 Study of events, processes and results

Now that we have the basic building blocks for a more complete model of information security management, with objectives, actors, resources, threats, and controls, it becomes possible to study what actually *happens* while managing information security. Therefore, a study of the events and processes of information security management would be interesting and beneficial for both theory and practice. For example, what happens when a control is so weak that a threat scenario becomes reality and affects the possibility of fulfilling the business and security objectives of an organisation? What do the different actors do, and why?

Following from this, another interesting and important avenue for research is studying the results of the application of different information security management practices, methods and standards. Questions such as: "Does an BS7799 certification result in a more efficient management system?", "Which is the most appropriate response to a confirmed intrusion?", and "In which way does the organisational environment affect the ideal approach to information security management?"

Appendix A

Paper D: “IFIP World Computer Congress (SEC 2000) Revisited”

This paper introduces a simple classification model for research in information security¹. The level of abstraction (‘theories and models’, ‘empirical world’) and domain (technical, formal, informal) are proposed as the key dimensions in the model. The 125 papers selected by international reviewers for presentation and publication at the IFIP World Computer Congress / SEC 2000 were analysed and classified according to the model, and the outcome of this effort is presented. The result is a high-level graphical view of the type of research that was presented in the SEC 2000 proceedings and at the conference in Beijing. Finally, we discuss the content of the congress with this view as our point of departure, aiming to identify areas that are well covered as well as areas that leave room for further advancement. As an appendix in this thesis, the paper serves two purposes: one, it illustrates the current trends and foci in information security research in a global context; two, it shows that the

¹This chapter is based on a previously published research paper (Björck and Yngström, 2001)

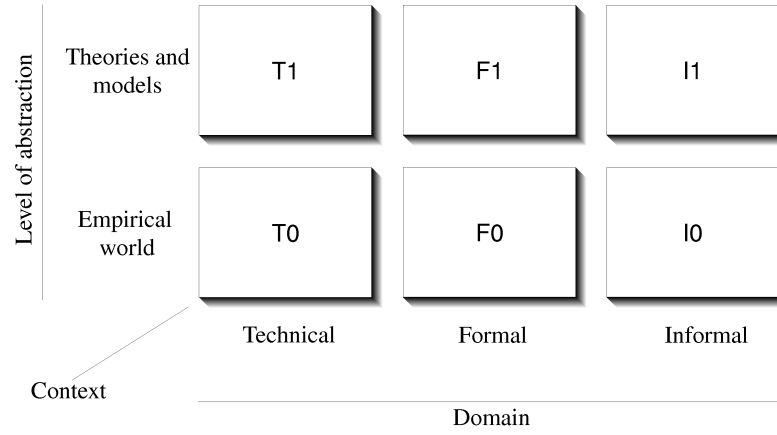


Figure A.1: A classification model for information security research.

subject tackled in this thesis – the management of information security in organisations – needs to be further investigated and researched.

A.1 The Model

Research in information security encompasses many different disciplines², competencies and focal points³. Moreover, it is of course possible to view the information security area from many different perspectives. Logically, the classification model presented here only represents one of innumerable potential views (figure A.1). The purpose of this model is to facilitate the analysis of research in information security by - for a

²Research in information security is carried out within the boundaries of many (reference) disciplines such as mathematics, computer science, social psychology, information science, criminology, etc.

³For example, some researchers in information security focus on computer systems, some on human activity systems, and others on privacy implications of information technology, etc.

given paper or other research contribution - showing the type of research reported on and within which domain it is positioned. The following subsections present the model, its origins and application in more detail.

A.1.1 Dimension X: Level of abstraction

This first dimension, ranging from *theories and models* to *empirical world*, caters to the need to distinguish between what is real and what is not. For example, the well-known Bell-LaPadula model specifies a multi-level security policy for a military computer system using mathematical notation and set theory (Bell and LaPadula, 1974). This model is an idea, a model, and a basic security theorem specifically concerned with the security of a technical system, and it would therefore be positioned in the T1 quadrant in the classification model proposed here (figure A.1). An existing access control system that *implements* the Bell-LaPadula model would be found in the empirical world, in the T0 quadrant in the classification model. Other models represent similar - but not necessarily identical - dimensions of information security with concepts such as:

- *Systems thinking* (models an ideal situation) and *real world thinking* offered by Soft Systems Methodology (Checkland, 1981), used in the area of information security by for example Fillery-James (1999).
- *Design/architecture*, *theory/model*, and *physical construction*, offered by General Living Systems Theory (Miller, 1978), used in the area of information security by Yngström (1996).

Focusing the variation in the level of abstraction is essential, since it helps us not only to detect if a given text reports on an idea, theory or model, or if it is concerned with artefacts in the physical world, but more importantly it helps us to see clearly if any attempts were made to move up or down in this dimension. In the case of the Bell-LaPadula model

used in the previous example, the process of implementing the model in a computer based access control system may be described as a deductive undertaking. Such a process can be represented in the classification model as an arrow from T1 to T0. Likewise, an inductive process can be illustrated with an arrow going in the other direction⁴.

A.1.2 Dimension Y: Domain

The *domain* dimension, ranging from *technical*, via *formal* to *informal*, originates from the work of Stamper et al. (1991)⁵. Other models represent a similar – but again, not necessarily identical – dimension of information and security with concepts such as:

- *Technical, operational, managerial, legal, and ethical* in the Systemic-Holistic Model by Yngström (1996)
- *Hardware, operating system, application, operational, administrative/managerial, political/legal, and ethical* in the Security By Consensus Model by Kowalski (1994).
- *Empirics, syntactics, semantics, pragmatics, and social world*. The three middle concepts are taken from the field of semiotics, originally introduced by Morris (1938). The two additional ones have later been proposed and described by a number of authors, for example Liebenau and Backhouse (1990)

The *technical* domain in the classification model (T0, T1) encompasses technical artefacts or ideas, models and theories about these (depending on the *level of abstraction*). Examples:

⁴Instantly recognisable deductive and/or inductive research approaches in information security might be relatively difficult to find. On the other hand, the model can be used also to illustrate the absence or combination of these and other research approaches.

⁵Dr. James Backhouse at the Computer Security Research Centre at the London School of Economics introduced these concepts (*technical, formal* and *informal*) and their usefulness within information systems security to the author in 1996.

1. computer hardware and software,
2. communication protocols and cryptographic algorithms,
3. technical evaluation methodologies,
4. *etc.*

The *formal* domain in the classification model (F0, F1) encompasses formal rules and procedures used to formalise human behaviour in an information system. *Formal* are those rules or procedures that are made explicit (usually - but not necessarily – *written*)⁶. Examples:

1. organisational information security policy,
2. legal system,
3. formal decision hierarchies,
4. *etc.*

Consequently, the *informal* domain in the classification model (I0, I1) encompasses informal human behaviour or ideas, models and theories about these. Examples:

1. social relations,
2. security implications of casual interpersonal communication,
3. ethics,
4. factual (as opposed to formal) organisational structures,

⁶Some might argue that software (such as operating systems, communication protocols, and applications) should be positioned in this *formal* domain, since they in fact consist of a set of formalised rules (the code). However, for the purpose of the proposed classification model in this paper, we have made the choice to distinguish between rules and procedures designed for humans and those designed for non-human processors, such as a CPU in a computer system. Thus, the formal domain only encompassed rules and procedures aimed at a human receiver.

5. power struggles,
6. *etc.*

By introducing this dimension, the classification model becomes more focused on research in information security within an organisational context. This may perhaps be an advantage, since it is in this setting that most information security services and products are demanded and will be used.

A.1.3 Dimension Z: Context

Context is added as a third dimension. Here, it originates from the systemic-holistic model (Yngström, 1996) where this factor is offered to cater to time and space. To continue the same example: the Bell-LaPadula model was presented in 1974 (time). It was concerned with the security of computer systems in a military setting (space).

This concludes the presentation of the classification model. Advantages and disadvantages of the proposed model are not further discussed in this paper. Nevertheless, some of these issues will most likely become apparent to the reader as we move on to applying the model in practice.

A.2 The Approach

The 125 papers from the IFIP World Computer Congress / SEC 2000 (Qing and Eloff, 2000) were analysed and classified according to the classification model proposed here.

This is a step-by-step description of how the examination and classification was approached:

1. Read all papers one by one and
 - a) extract and record the main focus,
 - b) extract and record the main contribution, and

- c)make a preliminary classification according to the model.
- 2.Read all papers for a second time and
 - a)extract and record the type of contribution,
 - b)note type of test or validation if performed, and
 - c)note if evaluation results were presented.
 - 3.Make a definitive classification according to the model.

The results were recorded in a simple spreadsheet to facilitate the awaiting statistical analysis.

Some of the information collected in the approach described above does not intuitively fit into the proposed classification model. Nevertheless, this information is needed for two reasons: firstly, to more exactly decide on the position of the paper in the model (for example within a quadrant); and secondly, to detect if attempts are made at “moving around” in the model (for example “Is this proposed technical computer system (quadrant T1) tested in a real-world setting (quadrant T0)?”).

There were no restrictions on the number of categories for the type of contribution or the type of test. However, after all papers were analysed, there were still no more than 12 *types of* research contributions and 6 *types of* tests recorded. Of course if we had preferred – and actively sought after – more narrow groupings, the effect would have been a more precise result, but also more categories.

A.3 The Result

First, a high-level view – using the proposed classification model (figure A.2) – of the 125 papers from the IFIP World Computer Congress / SEC 2000 (Qing and Eloff, 2000): Each dot in the figure represents one of the 125 papers. All dots that are positioned between an upper and a lower quadrant (within the dotted line) are those that involve some kind of movement in terms of level of abstraction (for example, testing a

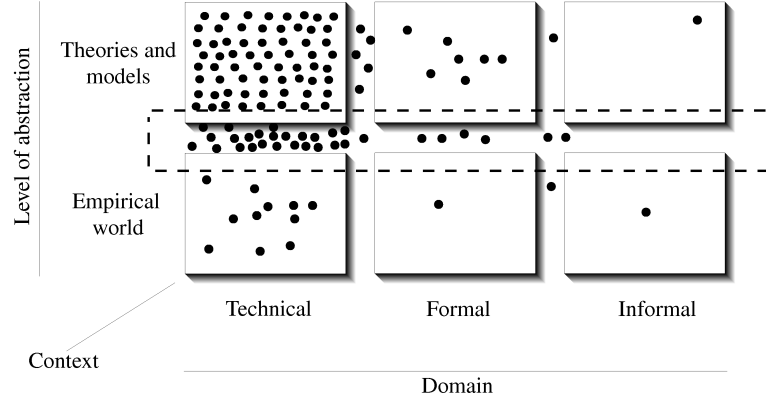


Figure A.2: Applying the classification model to the 125 papers from the SEC 2000 proceedings.

suggested approach by implementing it). Arrows indicating the correct direction should ideally have represented these papers, but due to space restrictions they are shown as dots here.

As can be deduced from studying the results shown in the classification model above, circa 104 of the 125 papers or 83% were of a technical nature, 14% of a formal nature, and 3% of an informal nature (please refer to the section describing the classification model, A.1, for a clarification of the concepts; technical, formal and informal). See figure A.3. That was the result from the horizontal analysis using the model. Let us examine the model vertically instead (results presented in figure A.4 below). Again, the 25% “moving” papers are those that involve some kind of movement in terms of level of abstraction (for example, testing a suggested approach by implementing it). The remaining papers, in total 75%, did not describe any such movements (figure A.4). *The most common type of contribution was described as an approach* (20%), followed by *discussion* (14%), *system* (12%), and *scheme* (12%)⁷. In total,

⁷This information cannot be derived from studying the results in the classification model; please refer to the section in this paper describing the research approach for

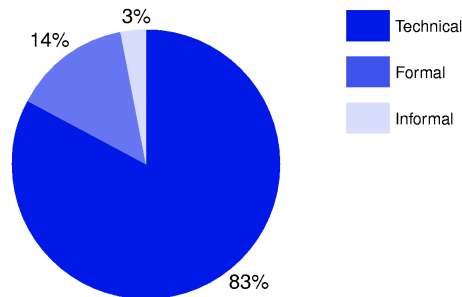


Figure A.3: SEC 2000; proportions of research papers in each domain.

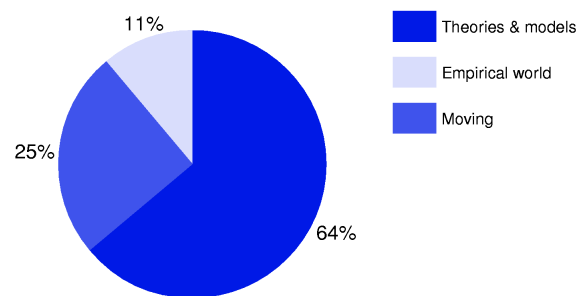


Figure A.4: SEC 2000; proportions of research papers at different levels of abstraction.

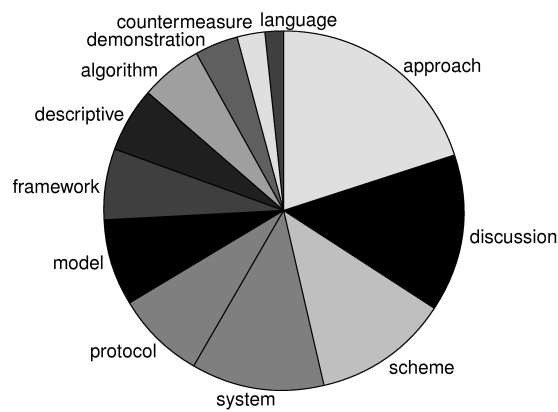


Figure A.5: SEC 2000; types of contribution.

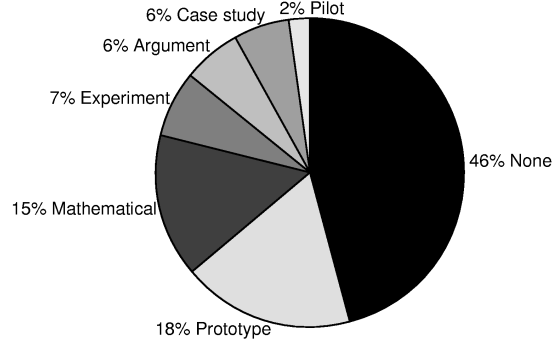


Figure A.6: SEC 2000; types of tests.

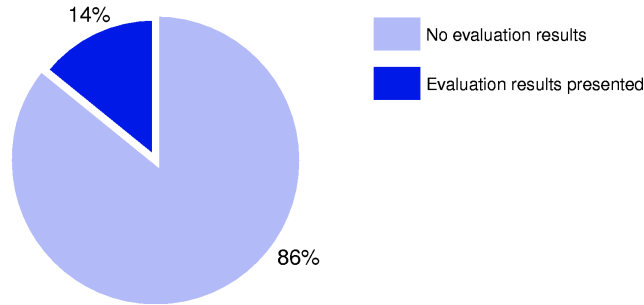


Figure A.7: SEC 2000; proportion of papers that contain evaluation results.

almost 6 out of 10 papers' contributions were of one of these four types (figure A.5).

Nearly half of the papers (46%) did not describe any tests *vis-à-vis* their conclusions. 18% tested the soundness of their findings by using a *prototype* and 15% by means of mathematical proof (figure A.6). This means that of the 66 papers that reported some sort of test, more than 6 out of 10 used either a prototype or mathematics to test their results.

Even though about 46% declared that they employed some kind of

more information.

1	Employee awareness	33,80%
2	Budget	27,10%
3	Human resources	25,40%
4	Management support	18,90%
5	Tools/security solutions	17,90%

Figure A.8: Greatest obstacles to addressing security concerns

test (figure A.6), only 14% of the 125 papers presented evaluation results (qualitative or quantitative) from such tests, as shown in figure A.7

A.4 The Discussion

More than 8 out of 10 analysed papers are focusing on technical issues, even though research and practical experience confirms that human behaviour - as represented by the formal and *informal* domains in the proposed model - largely affect the success of information security.

For example, a survey on computer crime based on answers from 1304 organisations with over 50 employees in Sweden found that employees' information security awareness is perceived as *the most important* means to overcome the security problems (Riksrevisionsverket, 1997). Another study, based on a survey about threats to EDP-stored information answered by 162 IT-managers, concluded: "The respondents consider the main threat against the organisations' EDP-stored information to be employees' unintentional and erroneous change and deletion." (Johansson and Kager, 1995) The result from Ernst & Young's Annual Global Information Security Survey (Ernst & Young, 1999), based on responses from over 4300 IT and executive managers in 35 countries, further underscores this line of reasoning (figure A.8).

The question was "Which of the following is the greatest obstacle to addressing security concerns?" Of the five obstacles listed in the survey questionnaires, tools and technical security solutions were seen as the

least significant obstacles, while employee awareness was seen as the primary challenge.

As mentioned, the analysis showed that more than 8 of 10 papers were focusing on technical issues. Technically oriented security research (and solutions) are crucial, since they lay the foundation for the secure operation of information and communication technologies. But today, as now evident, the critical problem is to be found elsewhere – in the *formal* and *informal* domains of the classification model.

A.5 The End

The main contribution of this paper was to propose a classification model for information security research. This model was subsequently applied to the 125 papers published in the proceedings of the IFIP World Computer Congress / SEC 2000. The main result of this analysis was the identification of an inconsistency between the current problems regarding information security in organisations today on the one hand and the focus of the 125 presented papers on the other hand. This outcome suggests that more emphasis should be placed on research on issues in the formal and *informal* domains such as information security education, the management of information security, ethics in information security, information security management systems, information security awareness and information security policies.

Appendix B

Report in Swedish: ”Revisorerna om införande och certifiering av LIS”

B.1 Bakgrund

På uppdrag av SIS’ LIS-projekt har Institutionen för Data- och Systemvetenskap vid Stockholm Universitet / KTH genomfört en kvalitativ enkätstudie syftande till att identifiera de erfarenheter och insikter deltagarna i projektets arbetsgrupp 3 erhållit beträffande införande och certifiering av ledningssystem för informationssäkerhet, LIS ¹

Genom att möjliggöra samarbete mellan informationssäkerhetskonsulter, revisorer, myndigheter (främst SWEDAC), och organisationer som söker certifiering, har arbetsgruppen sökt skapa och dokumentera unika erfarenheter. Syftet med denna rapport är att kommunicera dessa er-

¹Originalrapportens titel är ”Certifieringsrevisorernas perspektiv på införande och certifiering av LIS – en enkätundersökning”. Undersökning och rapport av Fredrik Björck som observatör i Projekt TK 099 ”Ledningssystem för Informationssäkerhet, LIS”, Arbetsgrupp 3 ”Pilotprojektet” (numera ”7799.nu”), SIS Standardisering i Sverige.

farenheter både inom och utom projekt LIS. Det torde finnas ett mycket stort intresse för detta, inte minst med tanke på att standarden nyligen blivit antagen av ISO som en internationellt erkänd standard, då med beteckningen ISO/IEC 17799:2000 (ISO, 2000).

Certifieringsrevisorernas och informationssäkerhetskonsulternas erfarenheter och insikter studerades i två separata studier. *Denna rapport beskriver endast resultatet från studien av revisorerna. Det finns en motsvarande rapport om konsulternas erfarenheter.*

I december 2000 nåddes en mycket viktig milstolpe för arbetsgruppen i och med att en av pilotorganisationerna blev tredjepartscertifierade enligt standarden. Därmed övergick arbetsgruppens fokus från att genomföra pilotcertifieringar till att dela med sig av alla de erfarenheter som skapats under de gångna åren. Denna studie och rapport är ett led i detta arbete.

B.2 Metod, demografi och reliabilitet

Undersökningen genomfördes som en skriftlig enkätundersökning med öppna frågor. Enkäten skickades ut till samtliga revisorer som deltagit i "pilotprojektet" (AG3) inom standardiseringsgruppens (STG) projekt TK099 – Ledningssystem för informationssäkerhet. Totalt kontaktades åtta respondenter med enkäten ($n=8$), och antalet svar efter en påminnelse slutade på sex, vilket ger en smält imponerande svarsfrekvens på 75% ($(6/8)*100$).

Generalisering utifrån resultatet är inte nödvändig, då det inte finns någon bakomliggande population vi önskar dra slutsatser mot. Undersökningen skall ses som ett försök till kartläggning av unika erfarenheter hos de personer som deltagit i ovan nämnda pilotprojekt. Det är således fråga om en totalundersökning av den föreliggande populationen.

Samtliga respondenter har mycket gedigen erfarenhet av certifiering, och 83% av dem var direkt involverade i en eller flera av de organisationer som sökt nå certifiering enligt 7799 (SIS, 1999b) genom pilotprojektet.

De tillfrågade lovades anonymitet i foljebrevet.

Vid några få tillfällen har svaren ändrats marginellt för att korrigera ett stavfel eller en grammatisk miss, eller för att förtydliga innebörden (ex. "enhet" har ändrats till "organisatorisk enhet"). Dessa ändringar har genomförts med stor försiktighet så att svarets semantiska innehåll inte har ändrats, utan snarare förtydligats.

Slutsatserna bygger på en strukturerad analys av det kvalitativa datamaterial svaren sammantaget utgör. Eftersom svaren samlats in elektroniskt från respondenterna minimeras de fel som annars ofta uppkommer vid inmatning på grund av överföring från ett media till ett annat (ex. vid avskrift av ljudupptagning för senare analys). Analysen av datamaterialet gick till så att varje svar (eller till och med *del* av ett svar) kodades med en kod som angav dess innehåll. Respondenternas olika svar på en given fråga (kontext) relaterades sedan till varandra med hjälp av koderna. Sakta växer då en modell (i det här fallet en visuell nätverksmodell) fram som visar likheter och skillnader i svar, samt som får oss att fokusera på det viktiga i svaren. Analysarbetet och den därpå följande induktiva processen (från enskilt svar via svarsmönster till slutsatser) underlättades av ett datoriserat metodstöd (ATLAS.ti), vilket gör det möjligt för andra att i efterhand kontrollera rimligheten i slutsatserna genom att undersöka vad – exakt vilka uttalanden/svar – respektive slutsats bygger på. En översiktsskiss som demonstrerar detta återfinns i slutet av rapporten.

Det har inte varit svårt att hitta gemensamma nämnare och mönster i svaren trots det låga antalet personer som deltagit i studien – tvärtom! Materialet visar på en närmast ofattbar samstämmighet, vilket ytterligare förvissar oss om att slutsatserna i föreliggande rapport är korrekta. Med korrekt skall förstås att; rapporten ger en riktig bild av hur de tillfrågade svenska revisorerna ser på de undersökta aspekterna beträffande införande och certifiering av ledningssystem för informationssäkerhet enligt 7799 (SIS, 1999b).

B.3 Framgångsfaktorer för införande

Den första frågan i enkäten till revisorerna löd:

*Vad anser Du vara de viktigaste faktorerna för ett framgångsrikt införande av ett ledningssystem för informationssäkerhet, LIS?
(motivera gärna svar)*

Ur svaren växte ganska omgående sex olika framgångsfaktorer fram. Eftersom samstämmigheten var så god väljer vi här att presentera svaren ordnade efter respektive faktor – i fallande ordning med den viktigaste, eller i vart fall den mest frekvent nämnda, faktorn först. Det kan vara värt att nämna att samtliga svar – hela materialet – föll under dessa sex faktorer utan ansträngning.

Framgångsfaktorer vid införande av LIS, ur revisorernas perspektiv, är följande:

B.3.1 Ledningens engagemang

Förankring i organisationens ledning, samt ledningens engagemang och förståelse för informationssäkerhetsproblematiken ansågs som den viktigaste faktorn för ett framgångsrikt införande av LIS. Denna faktor angavs först av samtliga, fastän enkäten inte hade några svarsalternativ och trots att respondenterna svarat ovetandes om de andras svar. Följande citat talar för sig själva:

”Ledningens intresse och aktiva engagemang i det egna LIS-projektet....”

”Ledningens engagemang och en förståelse för att ledningssystemet för informationssäkerhet måste omfatta hela verksamheten.”

”Ledningens engagemang...”

”Ledningens förståelse och engagemang, både i samband med fastställandet av säkerhetspolicy / säkerhetsnivå och att delta aktivt i riskbedömningen och avbrottsplaneringen.”

”Företagsledningens engagemang....”

”Förankring i företags/organisationens ledning....”

B.3.2 Välstrukturerat projekt

En annan viktig framgångsfaktor som identifierades är att projektet som skall införa LIS i organisationen är väl planerat och strukturerat. De olika respondenterna uttrycker sig så här:

”En organisatorisk enhet som ansvarar för helheten och för den riskanalys om ligger till grund för allt arbete....”

”...ett väldefinierat projekt med avgränsade delprojekt....”

Väl utarbetad projektplan och en rätt dimensionerad projektorganisation....”

Sammantaget är det flera olika aspekter rörande just organiseringen av själva arbetet med att skapa och införa ett LIS som tas upp:

- att helhetsansvaret för projektet är definerat,
- att det står klart *vem* som skall genomföra de olika delstegen i projektet
- att mål, medel och tidsplan för projektet är utarbetat och dokumenterat i en projektbeskrivning eller motsvarande, samt
- att resurserna i projektet – inte minst de mänskliga – är väl avvägda.

B.3.3 Holistiskt angreppssätt

Projektmedlemmarnas - och de övriga medarbetarnas - förmåga att se helheten betonas av flera av de tillfrågade som en viktig framgångsfaktor.

Det verkar bland revisorerna finnas en känsla av att de datatekniska aspekterna ofta hanteras ganska detaljerat, men på bekostnad av helhetssynen. Därför menar de att ett mer holistiskt angreppssätt och tänkande i projekten skulle medföra positiva konsekvenser och bereda väg för en framgångsrik implementering och eventuellt därpå följande certifiering av LIS. Två av de tillfrågade uttrycker det på följande sätt:

”...att de som deltar i arbetet med att ta fram risker är representanter för hela företaget, alltså inte bara för säkerhet utan även för andra delar av verksamheten.”

”förståelse för att ledningssystemet för informationssäkerhet måste omfatta hela verksamheten”

Som framgår av citaten är det främst kopplingen mellan informationssäkerheten och organisationernas kärnverksamheter som anses som viktigt – att LIS tar i beaktande och omfattar hela verksamheten – så att det inte stannar på säkerhets- eller IT-avdelningen.

B.3.4 Insikt om behov av informationssäkerhet

Att organisationerna inser behovet av informationssäkerhet är ytterligare en framgångsfaktor som identifierades:

”...att företaget ser ett behov av att skydda sin egen, kunders och andra intressenters information.”

”...förståelse för att ledningssystemet för informationssäkerhet måste omfatta hela verksamheten”

”Ledningens förståelse...”

Denna framgångsfaktor kan kanske anses som självklar. Trots detta nämns den vid flera tillfällen av de tillfrågade. Kanske indikerar detta att man ibland upplever en bristande förståelse avseende vikten av informationssäkerhet från delar av organisationen – kanske inte minst ledningsgrupperna.

B.3.5 Motiverade medarbetare

Några av delsvaren fokuserar på behovet av att motivera medarbetare:

”Att motivera de anställda till att arbeta fram processer och rutiner inom deras egna ansvarsområden....”

”...engagerad projektledare /-deltagare....”

Svaren tar främst upp vikten av att motivera personer som deltar i själva LIS-projekten, såsom projektdeltagare, projektledare, och ansvariga för olika delverksamheter i organisationen. Efter det att LIS skapats måste det också införas, och i det skedet växer vikten av denna framgångsfaktor – då skall *alla* medarbetare i hela organisationen motiveras att följa de regler och dagligen använda de tekniska lösningar projekten tagit fram och ledningen sedan beslutat.

B.3.6 Tillgång till extern kompetens

Den sista framgångsfaktorn som fångades upp i enkäten var just vikten av att kunna ta in extern kompetens där så krävdes:

”...bra bollplank (gärna certifieringsorgan från början).”

”... Tillgång till extern specialistkunskap.”

Det handlar då både om specialister och rådgivare inom informations- och IT-säkerhet, men även om att redan i ett tidigt skede öppna för en dialog mellan organisationen och certifieringsorgan. Denna kontakt – organisation *vs.* certifieringsorgan - måste ses som mycket viktig – inte minst om organisationen planerat att söka certifiering av sitt LIS efter införandet.

B.3.7 Sammanfattning

Genom analys av den kvalitativa enkätundersökningens svar från certifieringsrevisorerna inom projektet LIS, identifierades sex stycken framgångsfaktorer

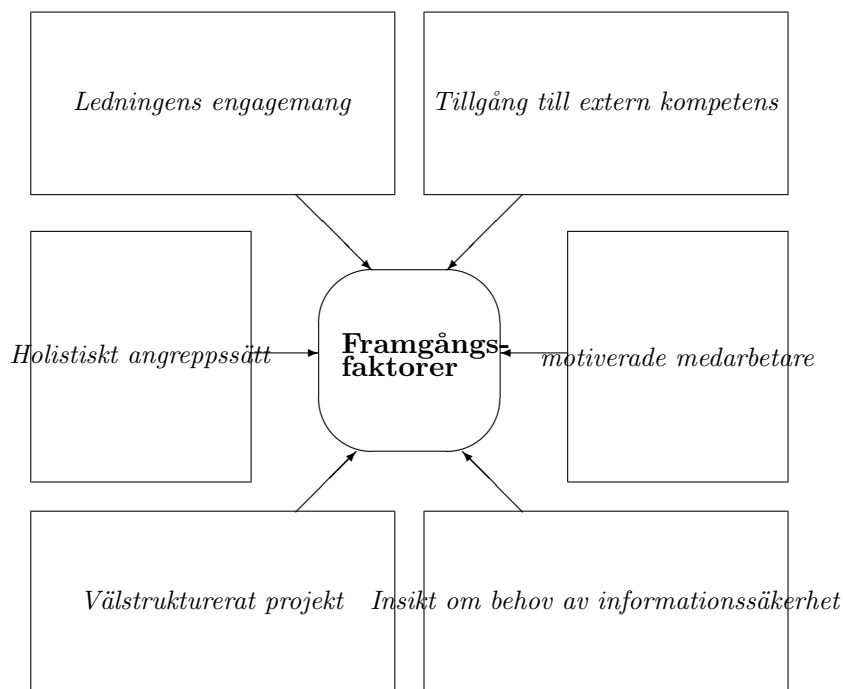


Figure B.1: Framgångsfaktorer för lyckat införande och certifiering av ledningssystem för informationssäkerhet enligt SIS (SIS, 1999b), ur certifieringsrevisorernas perspektiv.

med avseende på framgångsrikt införande av ett ledningssystem för informationssäkerhet. Eftersom certifieringsrevisorernas roll främst är att i efterhand kontrollera om ett ledningssystem för informationssäkerhet lever upp till kraven i standarden (SIS, 1999b), så är deras perspektiv en framförallt en betraktares, snarare än en utförares. Figuren ger en sammanfattande bild av certifieringsrevisorernas svar (figur B.1):

B.4 Svårigheter och utmaningar vid certifiering av LIS

Den andra frågan i enkäten till revisorerna löd:

Vad anser Du vara de största utmaningarna när det gäller certifiering av LIS enligt SS627799? (motivera gärna svar)

(”SS627799” i frågan åsyftar standarden som återfinns under referens SIS (SIS, 1999b) i referenslistan – det är den officiella svenska beteckningen på certifieringsdelen av standarden som brukar kallas ”7799”)

Ett utdrag av svaren:

”Utmaningen ligger inte i certifieringen utan i införsäljningen av budskapet att det är nödvändigt med en tredjepartsbedömning för att inte bli hemmablind!”

”Att få företagen att tänka över vilken information de behöver skydda. Viss information kan säkert ”läcka” utan att skada företaget.”

”Att få en förståelse för att ledningssystemet för informationssäkerhet skall omfatta hela verksamheten. Detta är svårt för många och visar sig exempelvis i samband med riskanalys, avbrottsplanering och i planering för incidenthantering.”

”Att se till helheten och förstå att det inte bara gäller IT utan till stor del andra delar det vill säga personal, skalskydd, etc. Att säkerställa att riskanalysen görs på ett för företaget korrekt sätt och att applicera den till företagets behov och utveckling, samt att den blir heltäckande.”

Svaren kan hänföras till tre olika problemtyper;

- ett *pedagogiskt* problem; hur *förklara* att LIS gäller hela verksamheten?,

- ett *marknadsföringsmässigt* problem; hur *övertyga* att certifiering ger mervärde?
- ch slutligen ett *metodrelaterat* problem; hur *säkerställa* att korrekt riskanalys genomförts?

Som en konsekvens av hur frågan är ställd ger egentligen svaren på frågorna inga svar – utan bara ytterligare frågor som kan, och kanske bör, tas upp för ytterligare diskussion. Här är en början på en diskussion kring de tre identifierade problemtyperna:

B.4.1 Overtyga att certifiering ger mervärde

Att låta tredje part intyga att ett LIS är effektivt och lever upp till kraven i 7799 (SIS, 1999b) kan medföra flera fördelar för en organisation. Problemet är att dessa fördelar inte nödvändigtvis gör sig tydliga för organisationen av sig själva. De kan se det så här: Om LIS redan är infört och om det redan fungerar, vilket är förutsättningen för en certifiering, så är ju redan informationssäkerheten god. Givetvis medför varje certifiering att problem upptäcks och kan åtgärdas, vilket i praktiken höjer informationssäkerheten. Om en höjning av informationssäkerheten är det *enda* som önskas torde dock en certifiering som åtgärd vara ganska dyrbar jämfört med en snabb nulägesanalys (med därpå följande åtgärder) av informationssäkerheten med hjälp av en informationssäkerhetsspecialist. Värdet av en certifiering blir således, ur detta perspektiv sett, främst att en oberoende tredje part intygar att LIS är implementerat, fungerar effektivt, och att det lever upp till kraven i 7799 (SIS, 1999b). Eftersom tjänsten – certifiering – främst är en försäkran för affärspartners och medarbetare, så är värdet av denna avhängigt *deras uppfattning* av värdet av ett sådant intygande. Denna uppfattning kommer att avgöras av hur skickliga certifieringsorganen är på att utföra certifieringarna, samt deras förmåga att kommunicera certifieringens fördelar för andra organisationer. Man kan också se det som självklart att en certifiering medför ett mervärde i och med att andra

parter kan lita på att vissa krav efterlevs. Detta synsätt förutsätter att det finns en någorlunda gemensam tolkning av standardens styrmedel och formkrav. Som sagt, frågan löses inte här – vi kan bara kontatera att detta är en av de utmaningar revisorerna ser.

B.4.2 Säkerställa att korrekt riskanalys genomförts

Revisorerna kommer ofta in i ett ganska sent skede – när LIS redan är infört. Detta gör att de genom att granska dokument från riskanalysprocessen måste kunna bilda sig en uppfattning av hur riskanalysen gick till och om den varit adekvat. Svårigheten ligger i att avgöra huruvida en given analys verkligen var fullgod, eller om det endast var rapporten om den som var välskriven. Omvänt gäller också att riskanalysen kan ha varit mycket effektiv, medans dess process och resultat av någon anledning blivit sämre dokumenterat. Sammanfattningsvis; utmängingen för revisorerna ligger i *att i efterhand säkerställa* att en korrekt och adekvat analys genomförts.

B.4.3 Förklara att LIS gäller hela verksamheten

Den sista gruppen av delsvar gäller det vi här valt att kalla den pedagogiska utmaningen; att förklara för personer i organisationerna att LIS gäller hela verksamhetens informationshantering och inte bara exempelvis den databurna informationen. Detta framkommer dessutom i svaren på såväl den första som den kommande frågan.

B.5 Fokus och tyngdpunkter i LIS-projekt

Den tredje frågan i enkäten till revisorerna löd:

Tycker Du att det (i det 7799-projekt Du tänker på eller generellt) funnits en bra balans vad avser fokus på datateknik-organisation, verklighet-dokument, produktivitet-säkerhet (eller andra dimensioner)? Finns det delar som överfokuserats eller aspekter som fokuserats för lite? (förklara gärna svar)

Ett utdrag av svaren:

”Bra i projektet men generellt tror jag att det finns en överfixering mot dataproblematiken, vilket gör att man missar delar av det övriga. Motmedel: följ standarden och skapa checklistor.”

”I det projekt som jag var involverad i var det huvudsakliga problemet att man bokstavligen läste standarden inantill och trodde att man var tvungen att uppfylla varje punkt utan att hänsyn till företagets behov (exempelvis med få lap-tops i företaget och inget behov att ta ut dem, så fanns det för närvarande inget behov av kryptering av hårddiskarna.”

”För mycket teknikorienterat. En tydligare fokus borde vara på helhetstänkande.”

”För lite fokus på affärsnytta, system och helhetstänkande och för mycket fokus på tekniska aspekter och nästan bokstavstrogen anpassning till standardens (del 1 av 7799) erfarenheter och förslag till styrmedel.”

”Generellt anser jag att de pilotföretag jag mött varit fokuserade på IT-säkerhetsperspektivet och inte på ledningssystemperspektivet och det vidare informationssäkerhetsperspektivet.”

”Vid våra sammanträden har ibland rena IT-frågor fått större vikt än övrig information. Under senare tid har mitt deltagande i sammanträdena och projektet varit begränsat.”

Analys av svaren ger vid handen att det främst är två skiften i fokus som önskas, sett ur revisorernas synvinkel:

- *Från* IT-fokusering *till* en helhetssyn på säker informationshantering, och
- *Från* Fokusering på standardens styrmedel *till* införande av relevanta åtgärder baserade på behoven och riskerna hos varje specifik organisation

I det följande diskuterar vi dessa två idéer.

B.5.1 *Från* IT-fokus *till* helhetssyn

Revisorerna upplever ofta att det finns ett obalanserat fokus och intresse för just IT-frågorna medan andra mjukare frågor som organisation, informationsklassning, och policies kommer i sista hand. Detta faktum har framkommit och kommenterats i tidigare frågor i undersökningen.

B.5.2 *Från* standardfokus *till* behovsfokus

Det verkar vara en missuppfattning att standardens krav skall gälla generellt för samtliga organisationer, eller i vart fall att de allra flesta av de styrmedel som föreslås där skall införas för att en lyckosam certifiering skall vara möjlig. Så är inte fallet, vilket respondenterna påpekar. Det är till och med så att en organisation som blint inför alla de krav som anges i standarden utan att redogöra för behovet av detta kanske *inte kan* bli certifierat. Det kan finnas andra krav som ligger utanför standarden men som måste införas, liksom att det kan finnas kompenserande kontroller i form av styrmedel liknande de som beskrivits i standarden, som måste införas. Vidare förekommer det givetvis att vissa styrmedel, eller till och

med hela grupper av styrmedel, i standarden inte är tillämpliga på grund av en organisations speciella risksituation. Ett enkelt exempel är att den organisation som inte har någon koppling till Internet naturligtvis inte behöver någon brandvägg för att skydda sig mot intrång via Internet. För organisationen handlar det alltså om att:

1. välja *ut* de styrmedel i standarden man *behöver*,
2. välja *bort* de styrmedel i standarden man *inte* behöver
3. *lägga till* andra styrmedel som inte återfinns i standarden men som krävs för en adekvat informationssäkerhet
4. *Valet av* både de valda och de bortvalda styrmedlen (enligt 1, 2 och 3) måste motiveras i ett så kallat "uttalande om tillämplighet". Dessutom måste utvecklingen och införandet av varje styrmedel anpassas till en för organisationen relevant nivå. Denna anpassning sker, vare sig man vill eller ej, i och med att styrmedlen konkretiseras i organisationen utvecklings- och införandefaserna.

Sammanfattningsvis; respondenterna ger uttryck för vikten av att fokusera mer på behovet av informationssäkerhet för en given organisation, än – vilket nu ofta är fallet – på det exakta innehållet i standardens exempel på styrmedel (även om dessa tjänar som en bra mall). Ett behovsanpassat LIS innebär inte bara att ledningssystemet kommer att bestå av andra kontroller än exakt de som återfinns i standarden, utan även att varje styrmedel måste anpassas och införas så att de erbjuder en relevant nivå av säkerhet för organisationen. Om båda dessa utmaningar lyckas kan organisationen erhålla certifiering.

B.6 Övriga kommentarer

Fjärde och femte frågorna i enkäten till revisorerna löd:

Vilken är den viktigaste kunskapen Du har idag gällande LIS – och då specifikt certifiering, som Du skulle vilja berätta för andra som står i begrepp att skapa, införa och sedan certifiera ett LIS enligt SS627799?, samt

Övrigt: Finns det något annat som Du vill ha sagt?

Vi presenterar här avslutningsvis endast *några* av svaren på dessa uppsamlingsfrågor utan vidare analys eller diskussion av dessa:

B.6.1 Tips till den som står i begrepp att skapa, införa och certifiera ett LIS

”Gå utanför IT-sfären, samt tänk på att de dokumenterade kraven ska fungera i verkligheten.”

”Se till helheten och affärsnyttan.”

”Att inse att riskanalysen som görs är en grund, grundval och utgångspunkt för att överhuvud taget kunna införa LIS”

”Klargör tydligt syftet med införande av LIS och se systemet som ett hjälpmedel att nå den fastlagda säkerhetspolicyn / säkerhetsnivån”

”Vikten av en väl genomförd, strukturerad och dokumenterad riskanalys.”

”Att i ett tidigt skede i projektarbetet förbereda åtgärder för upprättandet en kontinuitetsplan. Att ha en utvecklad metodik för uppbyggnad och införande av LIS.”

B.6.2 Övriga kommentarer

Ett utdrag av svaren:

”Standarden är otydlig i vissa avseenden är, men det krävs ännu mycken tolkningarfarenhet för att så småningom få en bra standard med rimlig efterlevnad.”

”Standarden, med skall-krav och best praxis kan verka förvirrande först. Många har inte tid att sätta in sig i standardens utformning utan vill ha ett snabbt svar och utgångspunkt att införa LIS. Det finns idag färdiga data-system som företagen kan köpa, som från dag 1 har färdiga kvalitetssystem. De behöver egentligen inte göra någon anpassning alls till sina egna processer. Denna utveckling är oroande. Om företagen köper denna gräddfil, kommer de att få stora problem vid certifieringen och fortlöpande problem vid uppföljande revisioner. Det är viktigt att stöta och blöta igenom alla problem inom företaget och se hur systemet kan växa fram och få växtkraft innan det kan utsättas för en oberoende tredje-parts granskning.”

”Vi måste alla betona för företag/organisationer betydelsen av att ha och inte ha ett system för hantering av informationssäkerhetsfrågor, att inte underskatta tiden det tar att ta fram och implementera systemet samt betydelsen av en opartisk bedömning.”

”Önskvärt att mer diskutera synen på medarbetare och deras kompetens, både som tillgång och hot. Standarden är här otydlig och tar egentligen inte hänsyn till serviceorganisationer och speciellt då kunskapsföretag”

Appendix C

Report in Swedish: ”Konsulterna om införande och certifiering av LIS”

C.1 Bakgrund

På uppdrag av SIS’ LIS-projekt har Institutionen för Data- och Systemvetenskap vid Stockholm Universitet / KTH genomfört en kvalitativ enkätstudie syftande till att identifiera de erfarenheter och insikter deltagarna i projektets arbetsgrupp 3 erhållit beträffande införande och certifiering av ledningssystem för informationssäkerhet, LIS¹.

Genom att möjliggöra samarbete mellan informationssäkerhetskonsulter, certifieringsrevisorer, myndigheter (främst SWEDAC), och organisationer som söker certifiering, har arbetsgruppen sökt skapa och dokumentera unika erfarenheter. Syftet med denna rapport är att kommunicera dessa

¹Originalrapportens titel är ”Informationssäkerhetskonsulternas perspektiv på införande och certifiering av LIS – en enkätundersökning”. Undersökning och rapport av Fredrik Björck som observatör i Projekt TK 099 ”Ledningssystem för Informationssäkerhet, LIS”, Arbetsgrupp 3 ”Pilotprojektet” (numera ”7799.nu”), SIS Standardisering i Sverige.

erfarenheter både inom och utom projekt LIS. Det torde finnas ett mycket stort intresse för detta, inte minst med tanke på att standarden nyligen blivit antagen av ISO som en internationellt erkänd standard, då med beteckningen ISO/IEC 17799:2000 (ISO, 2000).

Informationssäkerhetskonsulternas och certifieringsrevisorernas erfarenheter och insikter studerades i två separata studier. *Denna rapport beskriver endast resultatet från studien av informationssäkerhetskonsulterna. Det finns en motsvarande rapport om revisorernas erfarenheter.*

I december 2000 nåddes en mycket viktig milstolpe för arbetsgruppen i och med att en av pilotorganisationerna blev tredjepartscertifierade enligt standarden (SIS, 1999b). Därmed övergick arbetsgruppens fokus från att genomföra pilotcertifieringar till att dela med sig av alla de erfarenheter som skapats under de gångna åren. Denna studie och rapport är ett led i detta arbete.

C.2 Metod, demografi och reliabilitet

Undersökningen genomfördes som en skriftlig enkätundersökning med öppna frågor. Enkäten skickades ut till samtliga informationssäkerhetskonsulter som deltagit i "pilotprojektet" (AG3) inom standardiseringsgruppens (STG) projekt TK099 – Ledningssystem för informationssäkerhet. Totalt kontaktades arton respondenter med enkäten ($n=18$), och antalet svar efter *en* påminnelse slutade på tretton, vilket ger en svarsfrekvens på 72% ($(13/18)*100$).

Generalisering utifrån resultatet är inte nödvändig, då det inte finns någon bakomliggande population vi önskar dra slutsatser mot. Undersökningen skall ses som ett försök till kartläggning av unika erfarenheter hos de personer som deltagit i ovan nämnda pilotprojekt. Det är således fråga om en totalundersökning av den föreliggande populationen.

Samtliga respondenter har mycket gedigen erfarenhet av informationssäkerhetsarbete, och flera av dem var direkt involverade i en eller flera av de organisationer som sökt nå certifiering enligt 7799 (SIS,

1999b) genom pilotprojektet. De tillfrågade lovades anonymitet i följebrevet.

Slutsatserna bygger på en strukturerad analys av det kvalitativa datamaterial svaren sammantaget utgör. Eftersom svaren samlats in elektroniskt från respondenterna minimeras de fel som annars ofta uppkommer vid inmatning på grund av överföring från ett media till ett annat (ex. vid avskrift av ljudupptagning för senare analys). Analysen av datamaterialet gick till så att varje svar (eller till och med *del* av ett svar) kodades med en kod som angav dess innehåll. Respondenternas olika svar på en given fråga (kontext) relaterades sedan till varandra med hjälp av koderna. Sakta växer då en modell (i det här fallet en visuell nätverksmodell) fram som visar likheter och skillnader i svar, samt som får oss att fokusera på det viktiga i svaren. Analysarbetet och den därpå följande induktiva processen (från enskilt svar via svarsmönster till slutsatser) underlättades av ett datoriserat metodstöd (ATLAS.ti), vilket gör det möjligt för andra att i efterhand kontrollera rimligheten i slutsatserna genom att undersöka vad – exakt vilka uttalanden/svar – respektive slutsats bygger på. En översiktsskiss som demonstrerar detta återfinns i slutet av rapporten.

Det har inte varit svårt att hitta gemensamma nämnare och mönster i svaren trots det låga antalet personer som deltagit i studien – tvärtom! Materialet visar på en närmast ofattbar samstämmighet, vilket ytterligare förvissar oss om att slutsatserna i föreliggande rapport är korrekta. Med korrekt skall förstås att; rapporten ger en riktig bild av hur de tillfrågade svenska informationssäkerhetskonsulterna ser på de undersökta aspekterna beträffande införande och certifiering av ledningssystem för informationssäkerhet enligt 7799 (SIS, 1999b).

C.3 Framgångsfaktorer för införande

Den första frågan i enkäten till informationssäkerhetskonsulterna löd:

*Vad anser Du vara de viktigaste faktorerna för ett framgångsrikt införande av ett ledningssystem för informationssäkerhet, LIS?
(motivera gärna svar)*

Till skillnad från certifieringsrevisorerna (vilka fokuserade på *faktorer*), så fokuserade konsulterna mer på vilka *egenskaper/kunskaper* det enskilda projektet bör ha för att lyckas. Att arbetet med att skapa, införa och certifiera ett LIS bäst sker i projektform verkar därmed också vara en allmän mening bland konsulterna.

Analysen gick till så att varje uttalande, 37 stycken, kodades i två steg – först helt ostrukturerat och utan fördefinierade kategorier. Resultatet blev följande 23 kategorier av uttalanden:

- ability to put policy into practice
- accurate analysis of preceding security situation
- active employee participation
- active project members
- appropriate project organisation
- backing from top management
- balanced policy grounded in reality
- clear aim from top management
- customer organisation participation
- documented business processes
- feasible implementation method

- identifiable business benefits
- implementation know-how for project leader
- insight and knowledge about security
- integration with existing management systems
- monetary resources
- project ability to influence IT development
- realistic cost estimation
- realistic time plans
- regular communication with stakeholders
- top management awareness
- top management involvement
- understanding the need for security

En systematisk analys av kategorierna ovan resulterade i att de grupperades i – ansågs tillhöra – sex mer abstrakta kategorier, nämligen:

- Projektadministrativ förmåga
- Kommenderande förmåga
- Finansiell förmåga
- Analytisk förmåga
- Kommunikativ förmåga
- Exekutiv förmåga

För en helhetsbild av hur de olika kategorierna hör ihop med dessa sex övergripande kategorier – se nätverksdiagrammet i slutet av denna rapport.

Den följande presentationen av undersökningsresultatet för denna fråga utgår från de sex kategorierna.

C.3.1 Projektadministrativ förmåga (project management capability)

Projekthanteringskompetens - eller projektets förmåga att administrera och organisera sig självt i strävan mot målet (infört/certifierat LIS) - ansågs som en av de viktigaste faktorerna för ett framgångsrikt införande av LIS. Följande citat talar för sig själva:

”... realistiska tidsramar...”

”... realistisk uppfattning om vad som krävs i form av tid...”

”En aktiv arbetsgrupp...”

”När ledningen väl beslutat om införande är det helt avgörande hur det projekt som skall införa LIS bemannas, organiseras, ges uppgifter, tilldelas resurser och genomför införandet.”

Den projektadministrativa förmågan innefattar bland annat, vilket framgår av citaten, att projektets organisatoriska struktur är avpassad för dess uppgift, att det är rätt bemannat för uppgiften, att projektets medlemmar är - och ges möjlighet att vara – aktiva, samt att projektplaneringen tidsmässigt är realistisk.

C.3.2 Finansiell förmåga (financial capability)

En annan viktig framgångsfaktor som identifierades är att projektet som skall införa LIS i organisationen har finansiell förmåga. De olika respondenterna uttrycker sig så här:

” Klar målättnings från företagsledningen, pengar,...”

”Realistisk uppfattning om vad som krävs i form av tid och kostnader m m”

”...väl tilltagna resurser...”

Sammantaget är det främst två olika aspekter rörande just finansieringen av själva arbetet med att skapa och införa ett LIS som tas upp:

- att finansiella medel har avsatts för projektet, och
- att det finns en realistisk bild av hur omfattande finansiella resurser projektet totalt kommer att förbruka.

C.3.3 Exekutiv förmåga (executive capability)

Projektets förmåga att *omsätta dokument/idéer/regler i praktik* betonas av flera av de tillfrågade som en viktig framgångsfaktor. Förutsättningarna för denna exekutiva förmåga skapas med hjälp av flera andra kompetenser och förmågor:

- att projektledaren har erfarenhet från tidigare implementeringar av LIS,
- att man har en passande implementeringsmetod, eller i vart fall en idé om hur införandet skall gå till,
- att man har förmågan att omsätta det som står i informationssäkerhetspolicy och regelverk till praktik, och
- att man har möjlighet att påverka IT-drift och -utveckling inom organisationen (för att på så sätt införa informationssäkerhet den vägen)

Några av de tillfrågade uttrycker sig så här:

”... Att kunna fullfölja - från policy till parameter. Många jobb stannar på policynivån, där de ju inte gör någon nytta.

Policyn och standarden måste få effekt i det praktiska arbetet, och det är inte lätt. Tar antagligen år.”

”... framkomlig metod...”

”En aktiv arbetsgrupp som har... inflytande på IT-utveckling”

Projektets exekutiva förmåga är den som skall ta ledningssystemet från att vara ett dokument till att vara en beskrivning av en del av en verkligt fungerande verksamhet. I praktiken handlar det ofta om att man måste utbilda stora grupper medarbetare i organisationen för att åstadkomma förändring av beteenden så att det beskrivna ledningssystemet verkligen efterlevs.

C.3.4 Kommenderande förmåga (commanding capability)

Denna förmåga är direkt relaterad till den grad av uppbackning från organisationens ledning projektet erhåller. Uppbackning från ledningen beror i sin tur på ett antal faktorer såsom identifierbara affärsmässiga fördelar och ledningens förståelse rörande informationssäkerhetssituationen.

”Klar mållättning från företagsledningen...”

”Ledningens vilja och stöd... en organisation där det finns god förståelse för behov av säkerhet”

”Högsta ledningens förståelse och engagemang”

”Ledningen aktiva stöd då”

” Ledningens stöd vilket förutsätter affärsmässiga fördelar med att införa det”

Utan den kommenderande förmågan – innefattande rätten att i någon mån, å ledningens vägnar, ”ge order” till olika delar av organisationen - faller projektet platt.

C.3.5 Analytisk förmåga (analytic capability)

Några av delsvaren fokuserar på sådant som skapar förutsättningar för, och behovet av, en analytisk förmåga:

”Med erfarenhet från införande av andra ledningssystem är det oerhört viktigt att ha bra underbyggd nulägesanalys så att man kommer rätt från början.”

”Det gäller även här och viktigast är förberedande grundarbete och faktaunderlag till informationssäkerhetspolicyn, m.a.o. se till att ha en verklighetsförankrad policy och med rätt omfattning”

”... att verksamheten är processbeskriven eller motsvarande.”

”... att LIS är en del av befintlig verksamhetsstyrning...”

Det är den analytiska förmågan som skall hjälpa till att fånga upp den nuvarande (ursprungliga) situationen, och se vad som bör göras år den. Även integration med redan existerande regelverk, exempelvis ledningssystem för kvalitet och miljö, kräver analytisk förmåga om integrationen skall bli fruktbar.

C.3.6 Kommunikativ förmåga (communicative capability)

Den sista framgångsfaktorn som fångades upp i enkäten var just vikten av att kunna kommunicera med omgivningen på olika sätt. Detta skapar förutsättningar för aktivt deltagande från medarbetare i organisationen:

”Förståelse, vilja och engagemang från den verksamhet i vilken LIS skall införas”

”... att ständigt kommunicera och stämma av de olika delstegen”

”Den egna personalen måste medverka aktivt”

”Delaktighet från kunden”

Citaten ovan nämner främst sådant som den kommunikativa förmågan möjliggör. Det spelar ingen roll hur bra projektet är i övrigt om det saknar förmågan att kommunicera sitt budskap till omvärlden – organisationen. Den kommunikativa förmågan kommer till användning i alla faser i projektarbetet.

C.3.7 Sammanfattning

Genom analys av den kvalitativa enkätundersökningens svar från informationssäkerhetskonsulterna inom projektet LIS, identifierades sex stycken framgångsfaktorer med avseende på framgångsrikt införande av ett ledningssystem för informationssäkerhet. Figuren ger en sammanfattande bild av dessa (se figur C.1).

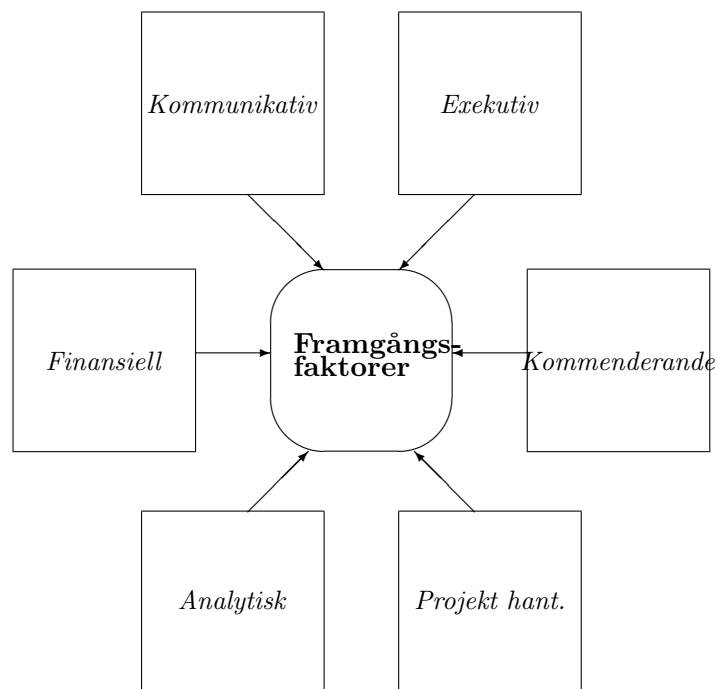


Figure C.1: Framgångsfaktorer för lyckat införande och certifiering av ledningssystem för informationssäkerhet enligt SIS (1999b), ur informationssäkerhetskonsulternas perspektiv.

C.4 Metoder och metodverktyg i 7799-projekt

Den andra frågan i enkäten till konsulterna löd:

Har Du i samband med 7799-projekt tagit hjälp av någon metod eller någon typ av metodverktyg, exempelvis för dokumenthantering, inventering av tillgångar, riskanalys, gap-analys, projektstyrning, eller annat? (Om ja, ange gärna vilka metoder och hur Du tyckte att det fungerade)

50% av de som besvarade frågan ($n=12$) har använt sig av en eller flera namngivna metoder eller metodverktyg för någon del av arbetet. Här följer en sammanställning av resultatet i tabellform (figur C.2).

<i>Metod / -verktyg</i>	<i>Källa</i>
Riskanalys	
CRAMM	www.ccta.gov.uk
RA Software Tool	www.aaxis.de
SBA Analys	www.dfs.se/sba
Nulägesanalys	
Bull Nulägesanalys	www.bull.se
Proteus	www.bsi-global.com
Projektstyrning	
PSM Projektstyrningsmodell	www.pejl.com
Assest management	
Comsecnordic ISMS 7799 TM	www.comsecnordic.se
Dokumenthantering	
BS5750:part 1:1979	www.bsi.org.uk
Doc Control	www.dokumentum.com
ITIL	www.itil.co.uk

Figure C.2: Metoder och metodverktyg

Ingen utav metoderna eller verktygen nämndes mer än en gång, vilket kan peka på att det ej ännu finns någon allmänt accepterad och vedertagen metod för konsulterna. De som inte har använt en namngiven metod har givetvis gått tillväga på något annat sätt – dvs använt en egen metod. SBA Check (www.dfs.se/sba - demo finns nedladdning), det av den Svenska Dataföreningen utvecklade svenska metodstödet för gapanalys mot bland annat 7799 nämndes inte av någon av konsulterna. Då SBA Check har runt 300 användare i Sverige då detta skrives så får man dra slutsatsen att användningen sker främst i andra sammanhang än i de undersökta certifieringsprojekten.

C.5 Fokus och tyngdpunkter i LIS-projekt

Den tredje frågan i enkäten till konsulterna löd:

Tycker Du att det (i det 7799-projekt Du tänker på eller generellt) funnits en bra balans vad avser fokus på datateknik-organisation, verklighet-dokument, produktivitet-säkerhet (eller andra dimensioner)? Finns det delar som överfokuserats eller aspekter som fokuserats för lite? (förklara gärna svar)

Ett utdrag av svaren:

"Det finns områden som inte tas upp som är mycket väsentliga för en organisation. Projektrutiner; hur och vilka faser skall beaktas i fråga om Informationssäkerhet då vi talar om projekt. Utan guidelines kan exempelvis en designer av hård/mjukvara fullkomligt demolera ett projekt genom att 'gjuta fel grund' och skapa en helt omöjlig situation för de som skal. Implementera säkerheten."

"Ja, bra balans."

"Egentligen inte (någon bristande balans) , men kanske vore ett bättre tydliggörande av ledningens ANSVAR som naglar fast den som chansar eller helt enkelt ger [tusan] i om olyckan drabbar företaget - vilket erfarenhetsmässigt är mycket vanligt. Kanske en juridisk fråga?"

"Eftersom jag själv styr detta är jag nöjd med balansen så långt. En ev certifiering kan naturligtvis tvinga oss till en annan fokusering som man inte är helt nöjd med."

"...jag tror att många kastar sig in i 7799-projekt utan att ha klart för sig vilken roll och betydelse IT har för verksamheten och hur IT är kopplat till affärs mål, strategi mm. Rätt svårt att prata säkerhet när vi inte riktigt vet vad som ska säkras!"

"Begreppen LIS Informationssäkerhetspolicy - säkerhetspolicy har varit något frustrerande att definiera t.ex en policy för datakommunikation som är gränsen mellan olika företags policies man vill begränsa det till den digitala överföringen men taga med legala aspekter som att det skall vara lagligt osv. Detta kanske är hämmande att man inte har kunskap om ISO 9000 utan fokuserar på IT-system."

"Ja, det finns en mycket bra grund att stå på för att visa att säkerhet inte 'bara' är en teknisk företelse, utan det är baserat på och är applicerbart just runt organisation och informationsflöde."

"Det beror på hur kunden ser ut."

"Nej! Många verksamheter fokuserar alldeles för mycket på tekniken. Förklaringarna kan var många. Min erfarenhet är att verksamhets-

cheferna har för lite kunskap om tekniken, vilket jag tror är på gång att ändras-det blir nog mer vanligt att f.d IT-chefer tar steget till att bli vd, och alltför gärna låter teknikerna få fritt spelrum. Vilken tekniker tycker om att dokumentera och sätta upp regler för sin verksamhet? Min uppfattning är också att det inte sällan klarlagts vilken nytta för verksamheten som IT-stödet skall utgöra."

"Det finns ett för stort fokus på själva certifieringen."

Analys av svaren ger vid handen att det främst är två skiften i fokus som önskas, sett ur konsulternas synvinkel:

- *Från IT-fokusering till en helhetssyn på säker informationshantering, och*
- *Från Fokusering på standardens styrmedel till införande av relevanta åtgärder baserade på behoven och riskerna hos varje specifik organisation*

Enkätundersökningen av certifieringsrevisorerna, vilken hade med exakt denna fråga, resulterade i liknande slutsatser (se gärna rapporten ”*Certifieringsrevisorernas perspektiv på införande och certifiering av LIS – en enkätundersökning*”, vilket är ett systemdokument till föreliggande skrift)

C.6 Övriga kommentarer

Fjärde och femte frågorna i enkäten till konsulterna löd:

Vilken är den viktigaste kunskapen Du har idag gällande LIS, som Du skulle vilja berätta för andra som står i begrepp att skapa, införa och certifiera ett LIS enligt SS627799?

och

Övrigt: Finns det något annat som Du vill ha sagt?

Vi presenterar här avslutningsvis endast *några* av svaren på dessa uppsamlingsfrågor utan vidare analys eller diskussion av dessa:

C.6.1 Tips till den som står i begrepp att skapa, införa och certifiera ett LIS

"Att man måste använda Standarden som ett ramverk där det krävs att man kompletterar denna med olika typer av del policys/ riktlinjer/ guidelines Och att man måste redan på ett tidigt stadium planera för att automatisera processerna samt uppföljning av dessa. Att inputen till regelverket kommer från människor som är verksamma inom respektive område. Tidigt även börja med utbildning av de olika grupperna som kommer att beröras"

"Fördelarna med att ha ett genomtänkt och fungerande ledningssystem."

"Att det är riskanalysen som avgör urvalet och nivån."

"Hur oerhört överlägsen en STANDARD inom det här området är jämfört med alla guldgrävande tyckande konsulter som var och en har sin egen ide om hur säkerhetsproblemen skall angripas (vilket även jag har). Faktum är att absolut inget har skett ifråga om infosäklning från det jag sysslade med detta"

på datainspektionen i 70-talets mitt och till 1995 när 7799 kom till.”

”Kanske att en grundbult är att identifiera och värdera/klassificera sina tillgångar (information, datorer, lokaler, försörjningsutrustning mm) så man vet vad som är skyddsvärt.”

”Låt inte 7799 överskugga allt annat. Bygg ett verksamhetssystem som passar ER, om det fungerar så bör rimligen 7799/9001/14001/17025/USK m fl.... falla på plats av sig själv”

”Aktivt deltagande”

”Att det finns enormt många godbitar att hämta även ifall man inte är helt mogen att ta ett helhetsgrepp för ett införande, utan att man kan välja och vraka bland de delar som är prioriterade för stunden och man har vetskapen att dessa delar kommer att passa in även i ett nästa steg. Att det skapas ett enhetligt vokabulär inom organisationer och även utanför dem är en förutsättning då fler och fler vill t.ex. benchmark’a sig. Certifieringen skapar en förståelse för hur stort området är och hur man kan angripa ett eventuellt införande.”

”Min erfarenhet från att arbeta i organisationer stora som små, att hantera relationer och andra verksamhetsrelaterade problem. Säkerhet är besvärligt för de flesta och det är väldigt viktigt att få en balanserad säkerhets anpassad just till aktuell verksamhet. Ibland är det vanligt att det blir ’för säkert’. En vanlig fråga bland yngre kollegor är eftergrågan av verktyg för att mäta vilken nytta som erhålls vid en viss vidtagen åtgärd. Min erfarenhet gör att jag har någotsånär lätt att utan verktyg uppskatta effekten av säkerhetshöjande åtgärder.”

”Var helt på det klara med varför ett LIS införs och varför det är viktigt att certifiera detta LIS. Finns det inte ett solklart mål samt att frågorna är besvarade och accepterade så är mitt råd att ’skynda långsamt’.”

C.6.2 Övriga kommentarer

”En sak som verkar ha stor betydelse för hur väl man lyckas är kvaliteten på den grunddokumentation som finns i företaget när processen startas. Detta har inte betonats tillräckligt.”

”Man skall vara ödmjuk inför en sådan här uppgift. Den är omfattande. Jag anser att man när det gäller risk/konsekvensanalys trampar in på ledningens område. Vi bör hålla oss mer specifikt till informationssäkerhet med IT-inriktning(Diskussionen har tidigare varit uppe!).”

”Kunder börjar nu efterfråga att leverantörer efterlever SS 62 77 99-standarden vilket kommer att vara påskyndande för införandet eftersom det då påverkar affärsmöjligheterna. Detta är betydligt mer drivande än om säkerhetsorganisationen föreslår ett införande, även om detta är välgrundat.”

”Jag anser väl att standarden är skapad endast med tanke på stora företag och myndigheters verksamhet, där det finns stora resurser att investera i åtgärder som krävs för att uppfylla standardens krav. Med resurser inkluderar jag att det oftast finns en speciell organisation som bara arbetar med detta. För en mindre verksamhet skulle jag önska en omarbeting av standarden som på ett enklare sätt kunde plocka fram de relevanta kraven. Eller ett tillägg till standarden som guidar ett mindre företag, säg mindre än 50 anställda.”

”Det skulle finnas ett antal förslag till Informationssäkerhetspolicy för olika branscher så att dessa skulle kunna vara det som förankras som modell först sedan modifiera beroende på HOT-bild och att arbetet läggs mer på riktlinjer.”

”En organisation, ett företag eller vilken verksamhet som helst har mycket nytta av att införa ett ledningssystem. Det måste dock vara väl avvägt till just aktuell verksamhet.”

Appendix D

Appendix D: How this research contributed to the software tool SBA Check

Early ideas for the graphical user interface for a revised version of SBA Check. This version is dated March 16 1999. This non-functioning design study was created using Borland Delphi – a rapid application development environment for Windows.

SBA Check I Företaget AB

Arkiv Redigera Navigera Rapport Hjälp

Aktuell kontroll

Sektion 1 Säkerhetspolicy

Avsnitt 1.1 Informationssäkerhetspolicy

Kontroll 1.1.1 Policydokument för informationssäkerheten

Fråga (1/109)

Har organisationen en av ledningen antagen övergripande informationssäkerhetspolicy? Är denna känd för de anställda? Har den ett adekvat innehåll? Efterlevs policyn?

Beskrivning av existerande kontroll

Företaget AB har ett övergripande policydokument i form av tre A4 sidor som beskriver mål, omfattning, efterlevnadskrav, samt konsekvenser vid överträdelse av policyn. Vidare hänvisar denna övergripande policy till mer konkreta riktlinjer.

Förbättringsmöjligheter

Eftersom de anställda känner till policyn och dess innehåll, men inte efterlever dess regler i någon större omfattning, rekommenderas någon form av informationsmöten och/eller utbildning om policyn riktad till de anställda. Denna utbildning

Bedömning

☐ Kontrollen finns och fungerar tillfredsställande

☐ Kontrollen finns ej, men det finns fullt kompenserande kontroll/er som fungerar tillfredsställande

☐ Kontrollen behövs ej av särskilda skäl

☒ Kontrollen fungerar ej tillfredsställande och/eller finns ej

Särskilda skäl

◀ ▶ Bästa Tillvägagångssätt

Figure D.1: Early design study of SBA Check

This version, from May 26 1999, is a primitive prototype. It was created in Microsoft Visual Basic, using Crystal Reports as its report generator component. This is the version that was included in the requirements specification, as a point of departure for the graphical user interface design. The 13-page requirements specification document was delivered from the research project to the Swedish Information Processing Society in June 7 1999.

SBA Check i Företaget AB

Aktuell kontroll

Domän	1	Organisation
Sektion	2	Informationssäkerhetspolicy
Kontroll	1	Policydokument för informationssäkerheten

Fråga
Har organisationen en av ledningen antagen övergripande informationssäkerhetspolicy? Är denna känd för de anställda? Har den ett adekvat innehåll? Efterlevs policyn?

Beskrivning av existerande kontroll
☐ Ej verifierad ☒ Verifierad
 Det finns en policy och medföljande handbok, men den var senast uppdaterad 1999.

Förbättringsmöjligheter
Uppdatera policy och regelverk för att reflektera den nya satsningen på Internet.

Bedömning

- ☐ Kontrollen finns och fungerar tillfredsställande
- ☐ Kontrollen finns ej, men det finns fullt kompensera kontroll/er som fungerar tillfredsställande
- ☐ Kontrollen behövs ej av särskilda skäl
- ☒ Kontrollen fungerar ej tillfredsställande och/eller finns ej

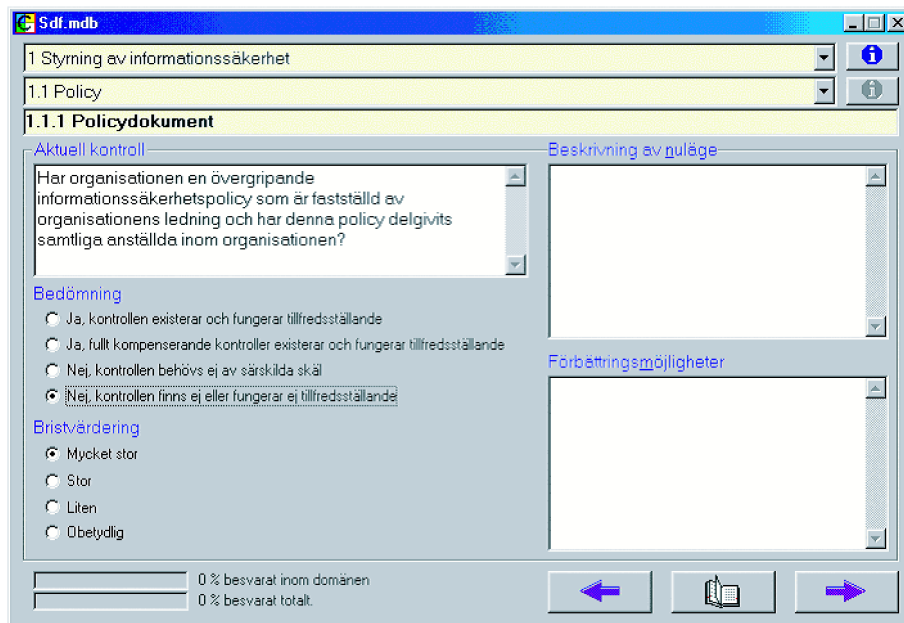
Prioritet

- ☐ Mycket betydande brist
- ☒ Betydande brist
- ☐ Mindre betydande brist
- ☐ Obetydlig brist

Bästa tillgängligssätt

Figure D.2: Primitive prototype of SBA Check

This screenshot, from August 27 2001, is from the current version of SBA Check (4.x). It was developed by the programmers at Eyetee AB in Microsoft Visual Basic, using Crystal Reports as its report generator component. As can be seen from the pictures, most of the core evaluation principles behind the tool, originated as a part of this research undertaking, are left unchanged through the years.



Sdf.mdb

1 Styrning av informationssäkerhet

1.1 Policy

1.1.1 Policydokument

Aktuell kontroll

Har organisationen en övergripande informationssäkerhetspolicy som är fastställd av organisationens ledning och har denna policy delgivits samtliga anställda inom organisationen?

Bedömning

☐ Ja, kontrollen existerar och fungerar tillfredsställande

☐ Ja, fullt kompenserande kontroller existerar och fungerar tillfredsställande

☐ Nej, kontrollen behövs ej av särskilda skäl

☒ Nej, kontrollen finns ej eller fungerar ej tillfredsställande

Bristvärdering

☒ Mycket stor

☐ Stor

☐ Liten

☐ Obetydlig

Beskrivning av guläge

Förbättringsmöjligheter

0 % besvarat inom domänen

0 % besvarat totalt

Figure D.3: Current version of SBA Check (4.x)

Appendix E

Thematic Interview Synopsis

E.1 Interviewee 01

E.1.1 Pressing need to explain IS/IT security to business executives

Interviewee 01 means that IS/IT security professionals have spent far too much time and energy discussing the definition of IS/IT security and what components it entails (e.g. confidentiality, integrity, availability - or also accountability?), while overlooking the pressing need to explain to top management what IS/IT security can potentially do for the business. Interviewee 01 illustrates this point with an anecdote from when he was director of security in one large multinational corporation: At a meeting with the corporate management team, it became clear that they thought that the concept 'integrity' referred to an individual's integrity, and it took some time for them to understand that the concept could also refer to integrity in e.g. the software code that is part of the products they sell. Furthermore, the management team's idea of IS/IT security was that it equalled confidentiality, and therefore they could not see that

they needed any of that, since they did not handle any confidential information. The successful management of IS/IT security requires that the IS/IT security manager uses a language that business executives can identify with. According to Interviewee 01, this language may well be based on more general risk management terminology.

E.1.2 IS/IT security is mainly concerned with protecting existing revenue streams

"Security is a competitive device." signed by, and with accompanying photo of, the CEO. Interviewee 01 recalls writing this personally, to be included in the first page of a book including the policies and directives of the corporation. Today the informant reasons otherwise: "I think one has a difficult journey if one expresses oneself like this, that: by way of investing in security - or considering the operating costs of security - we will be competitive. However, one can say that in order to be able to survive in the market, and in order to protect the balance sheet, we need these measures." In line with this, Interviewee 01 argues that IS/IT security can be viewed as being 'static' risk management, and for two reasons. First, it is (with very few exceptions) about protecting existing - rather than generating new - streams of revenue. Second, IS/IT security professionals are static in their perspectives on risk, in comparison with risk professionals in the insurance industry: "Insurers understand that they have taken on risk - they must know if the risk changes, while we [in IS/IT security] somewhere, I believe, assume that it is still a relatively stable world." Interviewee 01 illustrates this point by referring to an hypothetical organisation aiming for certification according to BS7799-2: If it is a large one, it has probably gone through several material changes from the time of the first internal evaluations, via implementation, to the time of the certification, and yet this dynamic is not well catered to in the methods we use.

E.1.3 Financial perspective needed in IS/IT security

Interviewee 01 argues that IS/IT security needs to adopt - and to some extent adapt - the tools, traditions, and competence that are available within the fields of business management and risk management. The common denominators of these are focus on the financial consequences of business decisions and events. An IS/IT security manager must therefore "... understand what a balance sheet is, what cash flow and income and loss statements are, and how it all fits together, to understand what the business risks look like." Interviewee 01 asserts that the current lack of a financial perspective in IS/IT security is mainly because of its military legacy: Firstly, IS/IT security originated in military environments with authors such as Bell and LaPadula. Secondly, many IS/IT security managers have a personal background in military or police organisations. In a doctoral dissertation, Interviewee 01 uses risk management tools as a "glue" between IS/IT security management and general business management.

E.1.4 IS/IT security needs to be decided economically and controlled technically

IS/IT security measures should ideally be built-in as technical controls in IT systems: "I believe that if one does not build it in, but expects that new employees, joint-venture partners, temporary workers, and contractors shall be able to read in a set of rules and then make an autonomous judgment on how they shall classify that information or that code, for that sake, that they temporarily sit down and work with - that does not work." Interviewee 01 means that such technical security controls should be enabled by default, based on a predetermined information classification scheme, so that the user does not need to make any decisions on what measures to use in a particular situation. The level of protection needed, and thus the information classification scheme, should be based on potential financial consequences of a security breach. In-

interviewee 01 suggests that one should approach this by a) identifying products/services that generate material revenue streams to the organisation; b) identifying potential scenarios of security breaches; c) identifying financial risk exposure, taking into account applicable insurance policies, and what types of risks they cover; d) identifying IT systems and personnel that are used to deliver these products/services; e) evaluating current security in the IT systems; f) deciding on the needed security level based on the financial risk exposure; and g) implementing the security level as technical controls.

E.1.5 Written IS/IT security instructions are mainly for the technical experts

Most written rules with regards to IS/IT security in an organisation should be geared towards technical experts working with the IT systems. They should use them e.g. when they are about to acquire or set up a new IT system for the organisation. Then they should look to these instructions and rules to see what security requirements they should implement in relation to what type of information the IT system will process. Other regular employees may have simple policy rules such as rules on how they are allowed to use the Internet and e-mail, "But nevertheless one shouldn't require employees read 200 pages on IS/IT security, or for that matter 50 or even 3 pages - I mean, they won't do it."

E.1.6 The objective for IS/IT security is ultimately to protect the balance sheet and cash flow

Interviewee 01 continues; "If we talk about a commercial business, then the objective for the IS/IT security efforts is to protect the business processes of the business and then ultimately to protect the balance sheet and the cash flow". To identify the balance between risk and profit, one must ask e.g. "How much do you earn on this service [or product]?"

What risks are inherent in the service [or product]?” Depending on the answer to these questions, one might choose to stop delivering a specific product or service or not to start delivering it in the first place. Alternatively, one might choose to devise some information security measures to mitigate the risks identified. According to Interviewee 01’s personal experience, top management’s perception of risk inherent in different business activities is not always aligned with reality: at times they perceive material risks in some areas, but after an evaluation it can be shown the risks were not that critical. And conversely: top management sometimes overlook the fact that new risks are created when old services are computerised or moved from a mainframe environment to a primarily Microsoft or UNIX and TCP/IP environment.

E.1.7 Forces affecting IS/IT security; owners, legal framework, reputation

Interviewee 01 argues in essence that money and financial matters are the main force that determines the context of and the requirements for the management of IS/IT security. This is not suggested as an ideal but is rather a conclusion from years of experience. Shareholders, legal requirements, and the importance of a good business reputation (goodwill) are the forces that are mentioned that put pressure on an organisation’s IS/IT security efforts.

E.1.8 Employees need to understand IS/IT security consequences of their own actions

Average users or employees in the organisation need to have enough knowledge to at least understand the (IS/IT security) consequences of their own actions and so that they can put forward what they require in terms of IS/IT security for their personal working environment. Interviewee 01 gives an example of a user who enters an agreement with a bank for Internet banking: the user needs to be able to understand

the technical security measures and risks associated with these as well as the legal framework surrounding the use of the service. Interviewee 01 concludes that this implies a need - and a market - for IS/IT security education and training.

E.1.9 IS/IT security can be managed, but only if you have identified the most important risks

Interviewee 01 mentions two main factors needed in order to be able to manage IS/IT security: identification of the most important IS/IT related risks to the business, and a language for communicating these risks with top management. IS/IT security managers could learn this from looking at other areas such as general risk management and auditing. Money, personnel, and a clear mandate from top management are resources needed for managing information security. These are often sorely lacking.

E.1.10 Main controls for IS/IT security; firewalls, intrusion detection systems, and anti-virus solutions

Businesses should work proactively with IS/IT security in order to stop problems before they occur. However, businesses need to be prepared if something happens, meaning that they can 1) detect problems; and 2) have countermeasures ready. Firewalls, intrusion detection systems, and anti-virus solutions were mentioned by Interviewee 01 as the most important measures in IS/IT security.

E.1.11 Information security should be concerned with all types of information regardless of media

Even paper-based information, telephone calls, facsimiles, et al. should be included in the management of information security. Interviewee 01 recalls that the management system he designed as a security manager included all of these (and more), which was good, since almost all

questions that came up were already answered in the security manual. However, Interviewee 01 is in doubt as to the cost-effectiveness of such a comprehensive security management system; "But to be self-critical, it was not worth the money - it doesn't work. I mean, you can build it into an IS/IT system like in the case with the value transport, but if you take it all the way, well then people should have encrypted mobile telephones. I mean, it doesn't work."

E.1.12 Largest threat is not the hacker, but mistakes

The largest problem in IS/IT security is the human factor: mistakes made by humans. For example a systems administrator or an outsourcing partner who makes a mistake, with possible breaches of business continuity as a consequence. Another form of human mistake in relation to IS/IT security mentioned by Interviewee 01 concerns unclear responsibilities e.g. in outsourcing agreements. Breaches in business continuity can damage not only your own business but that of your customers (which you may be held responsible for).

E.2 Interviewee 02

E.2.1 Adjusting security rationally

Interviewee 02's main contention is that in information security we often do not adjust security controls in a rational manner, with the consequence that these controls cause problems to employees in organisations. First of all, information security people tend to exaggerate a threat, explain it inaccurately (the threats and the controls), and have difficulties to adjust threats, security efforts, and behaviour to a rational working day.

Interviewee 02 illustrated the point with two real-life examples (one of physical access control to a building leading to "‘piggy-backing’" and one of access control to a web-based conference registration system leading to loss of customers). Both examples lead to the conclusion that as the threat is not explained to the people, the security controls appear annoying to them and lead to decreased productivity/efficiency. In addition, if people do not understand fully why the controls are in place, they tend to find ways to break the security.

The solution to the problem is that people that have to live with the security controls also have to think that they are important, and that they know that they are obliged to adhere to them. The solution is not new technology such as biometrics - people will still find ways of circumventing security if they do not want to follow the rules. Behaviour is key to security, not technology.

E.2.2 The role of the security manager

Continuing along the same line of reasoning, security managers often install all kinds of security measures (to protect not only the organisation but also themselves), but "‘The reality is that no one cares about it since no one understands it’". The role of the security manager should be to balance security: "‘This means you should never implement too much

security so you can no longer balance the risks against profitability and creativity”’.

The security manager should have the possibility and the responsibility to report directly to top management such as the CEO, but should use do so as infrequently as possible - only in emergencies and in other extremely urgent matters. If managers abuse the prerogative too often, they run the risk of not being heard in the future.

The security manager should not be responsible for ”‘information security”’ - this responsibility remains with those responsible for carrying out business activities. In this role the security manager should talk to those responsible and give reasons for security - but it is up to the other person to decide what to do.

E.2.3 The main threat is from the insider

More than 80% of the threats emanate from within the organisation, since it is much easier to *e.g.* access systems from within the local network. Also, because it is easier to break security and do it without being noticed from the inside, the consequences are also more substantial.

Sometimes security people tend to exaggerate the threat in general.

E.2.4 Defining IT security

”‘IT security”’ can refer to everything or nothing ”‘depending on which side of the table you are.”’ Just as in quality management, it can entail the management of the whole organisation or just a very small part of operations.

Interviewee 02 argues that ”‘information security”’ should not be viewed as an industry or a separate entity but rather as a function. Therefore, those responsible for a certain business activity are also responsible for the security in relation to it; it comes down to risk versus business opportunities. IT security is a business risk.

E.2.5 The power of good example

Using a number of examples, Interviewee 02 argues that if security is to be successful, we have to lead by good example. The first example is about the effects on the nurse of the medical doctor who is lax about the security of patient records (resulting in computer intrusion). The second example is about effects on other employees when the CEO brings his friends into a closed shop IT hall (in essence showing that it is 'OK' to break the rule that no one may enter without permission). The third example is about the CEO who shows openly that s/he cares about information security by having lunch with the security manager openly at the organisational monthly. All these examples back the contention that if manager want their subordinates to follow security rules, they have to be ready to follow them themselves.

E.2.6 Policy, Analysis, and Tools

For managing information security in organisations, one must have a policy, a risk analysis, and tools. The information security policy is often a single A4 page but broken down into more detailed security instructions (could be printed documents or on other media). The risk analysis needs to be aided by some kind of method that helps valuing the risks in economics terms and the tools to realise the security could be *e.g.* technically focused or that you try to change behaviour - organisational.

There is nothing magic about information security. Managing information security is no different than managing logistics or business accounting, even though the problems are different.

E.2.7 Security in a complex world

Interviewee 02 reasons that information security was simpler and more straightforward before, whereas the world we are trying to secure today is much more complex. "It's not that you can only - like before - lock the door; back then you could say "my terminals"." Today, there are

more entrances to each system and the roles of different actors are changing all the time. For example, some people might be enemies in some situations (business competitors) and in other situations it can be more rational and profitable to treat them as partners and friends in terms of information security. Thus the level of security needed constantly changes.

E.2.8 Relevant security depends on the business

Encryption of data and access control are not always the most important. In some situations (like in the example about hand-held devices in the health care sector) traceability is more important. The motive for security is connected to the type of business you are in.

E.2.9 In conclusion - people are key

”My message is very clear: Technology does not solve all problems. People are the key factor. The business is the other key factor. What is not in tune with the business, if people do not understand why it is necessary for the business, then it doesn’t work. It doesn’t matter what technology you have - there is no technology that can protect you against human beings - forget it.”. Interviewee 02 concludes that ”‘security that takes too much time or that costs too much is never implemented - even if the boss says ”‘Yes, we shall have it”’. And the boss will be the first to violate it.”’

E.3 Interviewee 03

E.3.1 On information security behaviour

To be able to change behaviour, one must understand the driving force behind behaviour. These driving forces can be different for different categories of employees and for different human beings. If you do not start with that and make sure people feel good and act in that direction, then it is very difficult to achieve a change in behaviour.

Interviewee 03 noted that sometimes it is easier to get people lower in the organisation to listen and then to get the top management interested in information security. The reason for this might be that top management can have other objectives such as economic as well as personal career considerations to take into account.

E.3.2 The importance of feedback

Feedback is an important management instrument in information security. Anything that is decided or implemented must be checked at a later stage by means of feedback reporting. It may happen that the resources are used for something other than the investment in security if people do not understand the need for it. Therefore it is important to increase the level of awareness by trying to explain the risks and point at what has happened and what might happen.

E.3.3 Using examples of security breaches

According to Interviewee 03, one efficient way of creating awareness of potential security risks is to illustrate them by using threats that have materialised in the past and resulted in real security breaches and consequences.

For each case where information security eroded, one find the cause. But and a good way to depict the risks is to say what can happen if you do not follow the rules, using the earlier incidents as illustrations.

E.3.4 Elements of efficient information security management

Efficient information security management entails good employee awareness of security, motivated employees, and top management support. In addition, employees should act in accordance with acquired awareness.

Different categories of employees need to have the information security message delivered in different ways, since they may have different reference points and different world views. As a security manager one must be a little bit of an artist and be able to understand how people view their world.

A unit manager for an operations unit or a development unit has to manage technology, personnel, environment, and administration. For all these, different security rules are needed. Thus, information security management takes place in all these areas.

The top manager in the organisation has to act in accordance with the security idea. One way of ensuring this is to start management efforts at the top management level: form their visions and objectives and then require their feedback.

E.3.5 The complexity threat

Interviewee 03 argues that the main threat to the security of information systems is not viruses or fires but rather their complexity. First of all you have the human being who is very complex in nature; then you have technology which is also very complex; and then you have the interplay between technology and human being. To this you have to add lack of skills in understanding systems, what happens in the systems, and what effects certain actions can have. Therefore it is extremely important that individuals in the organisation be responsible for tasks that correspond to their competence; otherwise their lack of competence can pose a security risk.

E.3.6 Information security cultures

Basic philosophies and cultures in organisations have a tremendous effect on information security. There are different kinds of security awareness and different types of security. Interviewee 03 contends that there is a significant difference in culture between a security organisation and other industries.

E.3.7 The relation between security and information security

Security and information security are quite similar. The security manager of an organisation and the information security manager have roughly the same tasks. However, the IT security manager has other tasks, such as security in technical systems.

E.3.8 Good information security starts with top management support

The most important and first task for any information security manager is to make sure the organisation's top management, the CEO or equivalent, is really backing security efforts. You have to be in agreement with top management of what is going to be done. Top management has to be the source of all directives that are sent out in the organisation. One way of assuring top management support is to explain the threats to them using stories about earlier materialised threats and incidents. In this way top management themselves will often be interested in taking initiatives for improved security.

E.4 Interviewee 04

E.4.1 Security equals quality

Interviewee 04 starts out by saying: "Let's start with my view of what security is." Security is quality. Quality is fulfilment of customer expectations (with regards to products or services) over time. Quality is achieved in a competitive environment which requires effectiveness (a relation between utility and resource - money, human capital, etc. - consumption). These activities take place in the context of conflict (between goals, means, and methods) in the organisation and in parts thereof. Interviewee 04 holds a systems view of the organisation, defining it in terms of inputs, outputs, and its interface to an outside environment. In order to manage these activities in conflict, there is logic and there is culture (which entails a fight between different organisational stakeholders). Interviewee 04 asserts that in (information) security, it can be difficult to manage these conflicts, partly because one is often not careful to define at which level (business processes, information about these processes, or the technology) these conflicts occur, or on which level a given problem exists. IT security efforts have no meaning unless they are mirrored in the business activities that take place. "IT is needed, because it is a part of the realisation of the business strategy and its requirements for quality and effectiveness."

E.4.2 Information security exists at different levels

One can view information security management on different levels (e.g. technology, information, business). Confidentiality, availability and integrity are most often seen as pertaining to the technology level only, although they should be seen to pertain to all three levels. The business level is (in systemic terms) quite unstructured - it is characterised by entropy. This lack of structure and order should be solved on the technical level - one should try to create neg-entropy, or structure. This

structure, as upheld by technology, is in principle unchangeable for the employee. Therefore it is important that it is the business level that tells the technology level what structure is needed and not the other way around. This is where information security management comes in - "information security: it affects our quality of products and services". In essence, Interviewee 04 argues that information security management offers a way to connect business needs (at the business level) with technology solutions.

E.4.3 Elements of information security - the security nexus

Interviewee 04 defines the management of information security as consisting of different parts. There is a policy which takes into account the view on quality and effectiveness. There is an organisation; there are employees. There is information technology, information system maintenance, and a physical environment. Interviewee 04 emphasises the need to make sure information security management is working not only in the information technology domain, but also on the level of information. In addition to the mentioned components, there needs to be some kind of control mechanism before a new information system is rolled out in the business - a so-called accreditation procedure. Furthermore, there needs to be some later control, after the information system is put into use, against the accredited level of information security.

E.4.4 Standards should be used to aid information security management

Interviewee 04 argues that standards, best practices, and tools should be used to aid information security management. It is Interviewee 04's experience that many think that data communication, IT and IT security are so new that there are no existing standards that can be applied to their problem. This view is often incorrect, and standards such as ITU E.800 (reliability), OSI (data communications (security)), Common

Criteria (secure systems evaluation), and ISO/IEC 17799 (information security management systems) can and should be used to solve problems in information security management. Interviewee 04 returns to the problem of which level should do what in security (IT, information, business), and argues that ISO/IEC 17799 could be used to make the business level think about what they need for the business, and thereafter to translate this to the lower levels.

E.4.5 The problem of delimiting the problem

When working with security one is forced to make decisions about what falls inside and what falls outside the scope of the work: "And then we have another thing that is difficult - to do delimitations! And when one shall do delimitation, then we have both: physical interface, we have an electronic interface, and we have an organisational interface." Delimitations are difficult, because they require making decisions.

E.4.6 Risk analysis should be conducted at the business level

Interviewee 04 holds a "quality-view of information security". In a discussion about major threats, he concludes that the lack of well-grounded analyses about information security, especially at the point of IT system acquisition, is the most critical threat to information security. Interviewee 04 argues that risk and vulnerability analyses should be conducted at the business level using the general quality requirements as a point of departure.

E.4.7 Threat identification using the OSI-model

Threats against information could be identified using the OSI-model - to discuss the implications of security problems at each level. The importance of certain information to the business should guide the effort to

identify threats - "‘which threats can exist against that the information fulfills what one wants it to fulfill?’"

E.4.8 Point of departure: Humans are assets, not threats

Interviewee 04 argues that we should start with the premise that "‘an insider’" is an asset. However, the situation around the individual can change his/her behaviour negatively, for example if pressured. Therefore, "‘we shall then expect that he, and sort of be careful with, to see what is needed for him to act *for* us rather than *against* us.’" These are safety factors; people who feel safe act in a good manner.

E.4.9 Relation between security in general and information security

Information security is not as concrete as security in general, which makes it difficult. One important relation between security in general and information security is that the latter protects information which pertains to the former. For example, the information about and on a certain (e.g. electronic) key used to lock an important door (general security) has to be protected by means of information security.

E.4.10 Requirements of information security

Interviewee 04 argues that the ISO/IEC 17799 standard which represents best practices for information security management systems is a good starting point for finding information security requirements. How these requirements should be met is however up to the situational context - if possible one should try to have quality requirements as a part of this (why do we require from this system)?

E.5 Interviewee 05

E.5.1 Information security managers should report to top management

Interviewee 05 noted that one of the main problems in information security management is that the information security manager often has a person above who acts as a gate-keeper and "filter" to keep the information security manager separated from both the ears and the resources of higher level management. Often this gate-keeper is the CIO or the CFO. The ideal situation to be strived for is where the information security manager can and will report directly to top management in the case of discovered security breaches as well as directly submit a complete annual or semi-annual report on the security situation.

E.5.2 How top management views security

Top management, continues Interviewee 05, often lack knowledge about information security. They tend to delegate the security problem to the IT department where they think it belongs. What they do not understand is that their information is often worth much more than the entire production machinery. Interviewee 05 takes an example from the medical sector where *e.g.* information about medicines can be very sensitive before patents are awarded, etc.

Therefore, the lack of knowledge about the value of information assets seems to be an important inhibitor for good information security. People know how to evaluate material assets - but not immaterial ones.

E.5.3 Finding the balance in security

The ideal situation is, according to Interviewee 05, when one knows the value of information assets and has decided how much one is willing to risk, and from that decides what to do in terms of security measures.

The value of information assets cannot be calculated exactly, but has to be approximated.

E.5.4 Information assets

The information assets that are supposed to be protected by information security efforts are usually in digital form. A part of these digital information assets are also available on paper. Information security is also about protecting these assets. Information classification seems to be problematic. Very simple classification schemes may work - schemes such as prohibiting a certain type of information from being sent via e-mail.

E.5.5 Information security is about risk management

Organisations have to decide what risks they are willing to take - this goes for any type of risk; business risks, information security risks, investment risks, foreign exchange risks, or whatever; but management often lack understanding in these areas today.

Another problem arises from information security managers who approach top management about what kind of antivirus program to acquire. That is not their task to decide on.

E.5.6 Management by objectives

Interviewee 05 prefers "management by objectives" when it comes information security management. Instead of concentrating on writing complicated and elaborate policy documents, the information security manager should concentrate on getting a change in the behavior of employees. So rather than writing detailed instructions about information security for different situations, departments, processes, and routines, you should try to work with getting security into the thinking about business processes.

Interviewee 05 does not think it is always necessary to have a documented management system or a documented system of rules to manage information security. Instead, education and training should be used as the primary tool to accomplish a change in employee behavior.

With education and training, information security awareness can also benefit other forms of information assets such as through verbal communication between employees and outsiders.

E.5.7 Analysis point of departure: Survival

When conducting risk analysis, Interviewee 05 starts out by talking about the factors that affect the survival of the business. Later these factors are broken down into scenarios depicting what could happen, the consequences, and then security measures.

E.5.8 The role of a security consultant

Interviewee 05 has noted that sometimes the role of the security consultant is to say to top management what the information security manager has tried to say for a long time. As it turns out, sometimes top management is more open to the external advice from an information security consultant than from the internal advice from a lower part in their own organisation. Interviewee 05 adds: "it is difficult to be a prophet in your own house".

E.5.9 In conclusion

Before, information security management was approached by writing large information security handbooks and documents. These are not used and no one cares about them. Documents should be kept to a maximum of 10 A4 pages if possible. Instead, one should try to focus on educational efforts.

E.6 Interviewee 06

E.6.1 The information security manager should report to the CIO

Organisationally the information security manager should be situated below the chief information officer, who in turn should report to the chief executive officer. The CIO's responsibilities are broader than those of an IT manager and include responsibility for all information in the organisation. The IT manager should also report to the CIO, which implies that the information security manager and IT manager are at the same organisational level.

E.6.2 Information security management starts with business planning and visions

Business plans and vision. Information security management takes as input the business plans and visions of the organisation. Business plans and visions set the direction for the security effort and also the overall level of security needed. The result of information security management on this level is an information security policy.

Objectives and strategies. On this level information security objectives and strategies are derived from business objectives and strategies. This level results in security requirements for different parts of the business as well as implementation strategies (e.g. how to conduct training, what type of information materials are needed, how to achieve the desired technical security, etc.).

Methodology choice. On this level the information security strategy is made operational. Here is decided e.g. whether the education and training should be produced in-house or via an external partner - if we for example have decided we need an intrusion detection system

(on the objectives/strategic level). Then we decide if we are going to acquire it and operate it ourselves or if we are going to outsource it - on the methodology level.

E.6.3 Information security awareness is needed

Employees need to understand why certain information security efforts are needed, otherwise they will not use them (e.g. Why is this secret? Why do I have to change my password regularly?). In addition, if employees do not understand where the organisation is going, it will be difficult for them to help develop the business in that direction.

E.6.4 Information security in practice in a critical public sector organisation

The organisation that Interviewee 06 consults for offers services which are critical to and can affect individuals' security and safety. Therefore, they have a baseline security process for all systems in place. In these processes, all systems are classified on a three level scale with regards to confidentiality, availability and integrity (for example, "1" means not important, "2" means somewhat important and "3" means a system that is extremely important).

The information security requirements (from the basic security process) for each system emanates from the laws and regulations that apply to that system and additional requirements as given by the basic security classification (each level in the classification entails a specific set of requirements based on laws and best practices, e.g. ISO/IEC 17799). The systems' adherence to these requirements is checked using checklist-based tools and consultant knowledge.

Security requirements for each system are then discussed with the system owner. The system owner is often also a unit manager.

The organisation subscribes to a service that provides information on new technical vulnerabilities that have a bearing on their systems.

In addition to the basic security process mentioned above, there is also an extended security process. Depending on the basic security classification, a system might have to go through the extended security process as well. This process requires a risk analysis to be conducted, usually using simple scales like '1 to 10' instead of monetary units. The risk analysis is scenario based and requires users, system owner, maintenance people, and an analysis leader to take part. This results in additional security requirements.

In the cases where secret security requirements for the system are not met, the system owner is given a timeline, for example three years, in which to adhere to all requirements.

E.6.5 A holistic approach to risk analysis is required

Interviewee 06 argues that one must approach risk analysis in a holistic fashion. This means that one cannot only do a risk analysis of one system as a separate entity if it is interconnected with many other systems, because of the inherent dependencies.

E.6.6 The role of the information security manager

The information security manager is responsible for deciding on the requirements in terms of information security, education, and training, and for ensuring that there are teaching materials available. There is also a responsibility for the information technology, for example that the firewall is in place if that has been decided. Another responsibility is auditing of systems so that they adhere to the security requirements. The information security manager should also be responsible for different types of analyses, for example security classifications, environmental analyses (what goes on in the security area in general, etc.). Another responsibility might be Tiger Teams.

E.6.7 Information security documentation should be kept to a minimum

Documents such as information security strategies, roads, and guidelines, should be kept to a minimum. They should be written in an easy to understand fashion and they should be pedagogical. If the overall information security policy is one page, it is almost certain it will be read. If it is three pages, it might be read. If it is twelve pages, it probably won't be read.

E.6.8 People and information security

Interviewee 06 does not view people as risks or threats at first hand. Instead they are people in need of training for information security. The employees who pose the largest threat are deemed to be the technicians, because they have a high access possibility and a thorough knowledge of systems.

There is also a specific role in security for top level management. Top management are mentors and models for the rest of the organisation; they have to set a good example.

E.6.9 Primary information security objective is employee awareness

The ultimate goal for information security efforts is to reach information security awareness among the employees. As Interviewee 06 puts it: "You can buy any number of machines, but if you do not have employee awareness, they'll put the password on a Post-It on the screen."

E.6.10 The main argument for information security is efficiency

Because of the dependence on information systems in many organisations, one can argue that information security can help employees to

work more efficiently. If the IT infrastructure "goes down", it costs money. Information security makes sure that the information and IT infrastructure are available when needed.

E.6.11 In conclusion

Information security management starts with the business plans, the organisation's economic situation, and its visions and ideas. So as an information security manager, Interviewee 06 argues, one could start with interviewing top management to get their views on information security, and then go on interviewing other groups of employees. And after that, the information security manager has to see what is already in place. The manager also has to take a good look at the organisation's competitors and thereby try to get the picture of the potential threats to information security emanating from these.

E.7 Interviewee 07

E.7.1 Focus in information security management systems

Interviewee 07 uses a "mindmap" to explore the meaning of information security management. At the heart of the mindmap is the management system, and around it questions that if answered will help to fill the concept of information security management (systems) with meaning.

The function of an information security management system (ISMS) is to verify and control risk and manage all information systems security efforts in the organisation.

The aim is to protect information resources, including applications, information, platforms (servers, clients), and networks. The identification of an information resource is also the first step in the information risk management methodology, called FIRM, that Interviewee 07 often employs in consulting assignments. Here it can sometimes be problems of concepts, e.g. 'what is a resource?'

The ISMS should be used by different actors on different levels in the organisation such as top management and CEO on the strategic level, the information systems security manager on the strategic and tactical levels, the IT manager on the tactical and operational levels, and the IT operations at the operational level. Interviewee 07 argues that although information security management takes place on all these levels, it is the strategic (and in some cases the tactical) level that is in focus when we talk about "information security management". However, the operational level directly affects the strategic level in that e.g. records of operational events (helpdesk incidents, IT system downtimes, etc.) will have to be fed into the planning process at the strategic level.

Information security management should be conducted through the application of methods and tools. What tools and methods should be used depend on the level (strategic, tactic, operative). It is important that these different tools employ a similar terminology, to avoid misunderstandings between the levels.

Moving over to the question of "when", Interviewee 07 discusses the frequency at which the information security management activities take place at the different levels: yearly (strategic), monthly/weekly (tactical), and daily (operational).

E.7.2 FIRM - an information risk management methodology

Interviewee 07 employs a risk management methodology known as 'FIRM' which stands for 'Fundamental Information security Risk Management'. When used on the strategic level, this methodology can be used when sitting down with top management once a year and going through the current information security situation in the organisation. The point of departure in this kind of analysis is to define an information resource, for example the e-mail system or a business application of some kind. The discussion starts with an analysis of the critical nature of the information resource in relation to the business. After that, the analysis focuses on level of threat, based on recent incidents over the preceding year. Questions such as the number and types (human, technical, software) of incidents and their consequences are answered. The idea of this methodology is to try to measure the risk level and get it down to an acceptable one. Interviewee 07 has been consulting clients with this methodology for about one year and concludes that it works very well. One important aspect of this methodology is in visualising the current level of risk, the potential impact, etc. This makes it a good communication tool for the information systems security manager to use with top level management.

E.7.3 Information security management is, in essence, risk management

Interviewee 07 goes on to state that information security management is and should be just risk management for the top management. There

are financial, operational, and market risks. The operational risks can be subdivided into personal, organisational, physical, environmental and informational risks. The CEO must manage all these risks and decide where to invest resources such as personnel. In order to do this successfully, the CEO needs a management system. The ability to identify and manage risks and opportunities is the difference between a good manager or board of directors and a bad one.

E.7.4 Elements of practical information security management

Information security management starts with an analysis of the current information security situation, how it is conducted, what rules are in place, and what incidents there are. This work can be aided by the 'FIRM' methodology. Once one knows the current situation, one can start to prioritize the different efforts - first acute efforts, and later strategic ones.

E.7.5 security is a part of quality

All information security efforts are really a part of the quality work because if you do not have security then you have a quality problem. Talking about quality and quality problems is also a good strategy to get time with the top management to discuss information security.

E.7.6 Too much focus on technology

It is still a common problem in many organisations that information security is approached from a technical perspective. Instead one should start from the risk management perspective. In essence, Interviewee 07 argues that information security should be based on business processes, economics, and management of risks.

E.7.7 Intentional and unintentional threats

Threats can be divided into for example intentional, unintentional, and acts of god. Intentional threats can emanate from inside the organisation or from outside. Unintentional threats are simple human errors caused by a lack of knowledge or poorly designed systems.

E.7.8 The role of motivation

Motivation is key to information security. It is about viewing everything as assets, viewing it as opportunities - that should be the point of departure. At the same time one should not forget that there are threats, also from the inside.

E.8 Interviewee 08

E.8.1 The information security function should ideally not be a part of the IT department

Interviewee 08 starts out by discussing the organisation of information security in a large public sector organisation (a group of companies/organisations), where he is IT security manager. The current organisational structure with regards to information security is that the IT security manager reports to the IT manager because the IT security function is a part of the IT department. This is not the ideal structure, since it does not guarantee the independence of the security function vis a vis IT operations. A good thing with the current structure is however that the IT security manager knows much of what is going on in the IT department, since he/she is a part of it. A better structure would be to have the IT security function directly under the board of directors, and reporting to the CEO (or the equivalent). Today the IT security function does not have any personnel but has a budget to hire consultants and to buy needed software support, etc. Being a group of companies, each organisation has its own appointed IT security coordinator (in total circa 50 persons). This is most often a person on a part-time basis only. They are often on a quite low level in their own organisation - it would be better if they were higher up and more known and respected. There are cases where the IT manager is also the IT security coordinator, which is less fortunate. In terms of financial resources, each organisation does not have any specific resources reserved for information security. Instead, this is taken out of the IT budget - which is a problem according to Interviewee 08.

E.8.2 Yearly information security themes

Interviewee 08 tries to inspire and motivate the security coordinators by having some kind of yearly theme for the information security efforts,

such as a drive for information classification, vulnerability analysis, etc. This is done through information and training.

E.8.3 Communication and feedback between the manager and the coordinators

Feedback and communication is done mainly on an informal basis. There is no formal instrument by which the coordinators have to report what they have done in terms of information security, so this reporting is done informally and on a continual basis. Nevertheless, information about *incidents* is collected and reported by the coordinators, so that the IT security manager has a good grasp of what is going on.

E.8.4 Requirements on information security

Being a public sector organisation, the requirements put on information security are mainly based on legal restrictions. This is also mirrored in the organisation's high-level information security policy: to identify and adhere to legal requirements, and to optimize the protection in relation to identified risks. One important aspect of information security is to protect the brand name of the organisation (to avoid "badwill"). There is also a more detailed policy available based on the 7799 standard. In addition to this, there are a number of documents with the good advice and instructions which relate to security. The detailed information security policy can be applied as it is in the local organisations. However, they also have the right to further specify the policy, or to enforce a higher level of information security. The total number of people affected by the work of the information security manager is over 100,000. There are 50,000 employees in the organisations, of which 35,000 are computer users. In addition, there are circa 80,000 students who use computers in schools run by the organisation. The number of computers involved approaches 50,000.

E.8.5 Challenges of the job

Interviewee 08 argues that the most difficult part of the job is to activate the people that have information security responsibilities.

E.8.6 The information security managers role

One of the main tasks of the information security manager is to acquire methods and techniques for supporting the information security efforts. The current toolset contains tools and methods for risk analysis, for benchmarking against best practice (iso/iec 17799), for documentation and incident handling, anti-virus protection and firewalls. In situations where the IT department is in the process of acquiring some information technology which relates to information security, then the information security manager is called in and asked to approve the choice. Sometimes the information security manager acts like a legal adviser internally, when there are questions about security and legal issues. Another part of the manager's role is to be a part of the planning of the annual IT audits (not the execution). The organisation's internal IT auditors use a standard audit methodology (SBA Check, iso/iec 17799).

E.8.7 Risks and threats

The main concern for the organisation in terms of information security mentioned by Interviewee 08 is the confidentiality of potentially secret information. Therefore, the risk of internal and external computer intrusions are mentioned as potential threats to security. Incidents such as mailbombing have resulted in loss of functionality (availability problem). Computer viruses are stopped to 99% (the organisation installed automatic virus updates). Another threat against information security is the theft of electronic devices such as flat LCD-screens. However this threat is deemed to be under control.

E.8.8 Authentication

As a part of the organisation's e-strategy, services related to the core information of the organisation should be made available via the Internet - for employees, citizens and businesses. An identification and authentication portal has been built to cater to the security needs. It is based on a three dimensional matrix; the sensitivity of the system, the point from which accesses to requested, and the resulting authentication method (ranging from passwords to smart cards).

Bibliography

- J. Adams. *Risk*. Routledge, New York NY, USA, 1995.
- R. Baskerville. Investigating information systems with action research. *Communications of the Association for Information Systems*, 2(19), 1999. Tutorial.
- D. Bell and L. LaPadula. Secure computer systems: Mathematical foundations and model. Technical Report M74-244, MITRE Corporation, Bedford MA, USA, 1974.
- F. Björck. The economics of information systems security. London School of Economics, Department of Information Systems, 1996.
- F. Björck. Information security survey sverige 1997. Technical report, Ernst & Young AB, Stockholm, Sweden, 1997. Based on 541 survey responses from Swedish IT- and Information security managers.
- F. Björck. Information security survey sverige 1998. Technical report, Ernst & Young AB, Stockholm, Sweden, 1998. Based on 428 survey responses from Swedish IT- and Information security managers.
- F. Björck. Auditing information security management systems - towards a practical method. In Q. S. and J. Eloff, editors, *IFIP/SEC2000: Information Security - Information Security for Global Information Infrastructures*, pages 102–104, Beijing, China, August 2000. International Federation for Information Processing, International Academic Publishers.

- F. Björck. Implementing information security management systems - an empirical study of critical success factors. In J. Eloff, L. Labuschagne, R. von Solms, and G. Dhillon, editors, *Advances in Information Security Management & Small Systems Security*, pages 197–211, Hingham MA, USA, September 2001a. International Federation for Information Processing, Kluwer Academic Publishers.
- F. Björck. *Security Scandinavian Style - Interpreting the Practice of Managing Information Security in Organisations*. Stockholm University / Royal Institute of Technology, Stockholm, Sweden, 2001b. Licentiate thesis.
- F. Björck and L. Yngström. Ifip world computer congress / sec 2000 revisited. In H. Armstrong and L. Yngström, editors, *WISE 2 - Proceedings of the IFIP TC11 WG 11.8 Second World Conference on Information Security Education*, pages 209–223, Perth, Australia, July 2001. International Federation for Information Processing.
- D. Brewer. Web site of gamma secure systems limited. <http://www.gammassl.co.uk>, 2000.
- British Standards Institute. Information security management, part 2: Specification for information security management systems. Technical Report BS 7799-2, British Standards Institute, London, United Kingdom, 1995.
- British Standards Institute. Information security management, part 2: Specification for information security management systems. Technical Report BS 7799-2, British Standards Institute, London, United Kingdom, 1999.
- Bundesamt für Sicherheit in der Informationstechnik. It baseline protection manual - standard security safeguards. Technical report, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, 2001.

- G. Burrell and G. Morgan. *Sociological Paradigms and Organisational Analysis*. Heinemann, London, United kingdom, 1979.
- P. Checkland. *Systems Thinking, Systems Practice*. John Wiley & Sons, Chichester, United Kingdom, 1981.
- F. Cohen. Viruses, corruption, denial, disruption and information assurance. In L. Yngström, editor, *Information Security - the Next Decade, Proceedings of the IFIP TC11 11th annual working conference on information security*, Amsterdam, Netherlands, 1995. Kluwer Academic Publishers.
- Computer Economics. Computer economics virus impact update. Technical report, Computer Economics, San Diego CA, USA, 2001.
- Computer Security Institute. Computer crime and security survey. Technical report, Computer Security Institute, San Fransisco CA, USA, 2001.
- C. Cresson Wood. Using information security to achieve competitive advantage. *Journal of Computers and Security*, 10:309–404, 1991.
- R. Cyert and J. March. *A Behavioural Theory of the Firm*. Prentice Hall, Englewood-Cliffs NJ, USA, 1963.
- W. E. Deming. *Out of the Crisis*. Massachusetts Institute of Technology Center for Advanced Engineering, Cambridge MA, USA, 1986.
- M. Denscombe. *The Good Research Guide*. Open University Press, Buckingham, United Kingdom, 1998.
- G. Dhillon. *Interpreting the management of information systems security*. PhD thesis, London School of Economics and Political Science, London, United Kingdom, 1995.
- M. Eloff and S. von Solms. Measuring the information security level in an organisation. In J. Eloff and R. von Solms, editors, *In Information*

- security - small systems security & information security management*, pages 16–30, Laxenburg, Austria, 1998. International Federation for Information Processing.
- M. Eloff and S. von Solms. Information security management: An approach to combine process certification and product evaluation. *Journal of Computers and Security*, 19(8):698–709, 2000a.
- M. Eloff and S. von Solms. Information security: Process evaluation and product evaluation. In S. Qing and J. Eloff, editors, *Information Security for Global Information Infrastructures*, Amsterdam, Netherlands, 2000b. International Federation for Information Processing, Kluwer Academic Publishers.
- Ernst & Young. Information security survey. Technical report, Ernst & Young LLP, Cleveland OH, USA, 1999.
- Ernst & Young. Information security survey. Technical report, Ernst & Young LLP, Cleveland OH, USA, 2001.
- Ernst & Young. Global information security survey. Technical report, Ernst & Young LLP, Cleveland OH, USA, 2004.
- T. Falk and N.-G. Olve. *IT som strategisk resurs*. Liber, Malmö, Sweden, 1996.
- H. Fillery-James. *A Soft Approach To Management of Information Security*. PhD thesis, Curtin University of Technology, Perth, Australia, 1999.
- V. Fååk. Unused tools are useless or why is the gap between theory and practice in network security so wide. In L. Yngström, editor, *Information Security - the Next Decade*, Amsterdam, Netherlands, 1995. International Federation for Information Processing, Kluwer Academic Publishers.

- B. Glaser. *Advances in the Methodology of Grounded Theory: Theoretical Sensitivity*. Sociology Press, Mill Valley CA, USA, 1978.
- B. Glaser. *Basics of Grounded Theory Analysis*. Sociology Press, Mill Valley CA, USA, 1992.
- B. Glaser. *Doing Grounded Theory: Issues and Discussion*. Sociology Press, Mill Valley CA, USA, 1998.
- B. Glaser and A. Strauss. *Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine, Chicago IL, USA, 1967.
- R. Glaser. Measuring the value of information: The information-intensive organization. *IBM Systems Journal*, 32(1):99–110, 1993.
- E. Guba. *Toward a methodology of naturalistic inquiry in educational evaluation (Monograph 8)*. UCLA Center for the Study of Evaluation, Los Angeles CA, USA, 1978.
- B. Gustavsson. *Metod: Grundad Teori för ekonomer*. Academia Adacta, Lund, Sweden, 1998.
- J. Highland. Perspectives in information technology security. In *Proceeding of Education and Society - Information Processing '92*, 1992.
- E. Humphreys. Draft bs 7799 part 2 (version d). Photocopied, 2001.
- Insight Consulting. Insight on cramm iv. Technical report, Insight Consulting Limited, Walton on Thames, United Kingdom, 2001.
- ISACF. *Control Objectives for IT and Related Technologies, COBIT*. Information Systems Audit and Control Foundation, IT Governance Institute, Rolling Meadows IL, USA, 1996.
- ISACF. *Control Objectives for IT and Related Technologies, COBIT*. Information Systems Audit and Control Foundation, IT Governance Institute, Rolling Meadows IL, USA, 3 edition, 2000.

- ISO. Iso/iec 17799:2000 - information technology - code of practice for information security management. Technical report, International Organization for Standards, Geneva, Switzerland, 2000.
- L. W. Jeter. *Disconnected: deceit and betrayal at WorldCom*. J. Wiley, Hoboken, N.J., 2003. Lynne W. Jeter. 24 cm.
- H. Johansson and M. Kager. Perceived threats against information in adp-systems. a study of swedish dp-managers perception. Master's thesis, Stockholm School of Economics, Department of Information Management, Stockholm, Sweden, 1995.
- F. Knight. *Risk, Uncertainty, and Profit*. Houghton Mifflin Company, Boston MA, USA, 1921.
- S. Kowalski. *IT insecurity : A multi-disciplinary inquiry*. PhD thesis, Stockholm University and Royal Institute of Technology, Department of Computer and Systems Sciences, Stockholm, Sweden, 1994.
- L. Labuschagne. Web assurance: Information security management for e-commerce. In J. Eloff, L. Labuschagne, R. von Solms, and G. Dhillon, editors, *Advances in Information Security Management & Small Systems Security*, Boston MA, USA, 2001. International Federation for Information Processing, Kluwer Academic Publishers.
- J. Liebenau and J. Backhouse. *Understanding Information: An Introduction*. Macmillan Press, London, United Kingdom, 1990.
- M. C. S. Lim. Barings futures (singapore) pte ltd: Investigation pursuant to section 231 of the companies act (chapter 50). Technical report, Singapore Ministry of Finance, 1995.
- Y. Lincoln and E. Guba. *Naturalistic inquiry*. Sage, Beverly Hills CA, USA, 1985.
- D. Longley and L. Kwok. A security officer's workbench. *Journal of Computers and Security*, 15(8):695–705, 1996.

- A. Marin. Cost and benefits of risk reduction. In *Risk: Analysis, perception and management*. Royal Society, London, United Kingdom, 1992.
- D. McGregor. *The human side of enterprise*. McGraw-Hill, New York NY, USA, 1960.
- Merriam-Webster. Perception. Online, December 2004.
- J. Miller. *Living Systems*. McGraw Hill, New York NY, USA, 1978.
- H. Mintzberg. *Structures in Fives: Designing Effective Organizations*. Prentice-Hall, Englewood Cliffs NJ, USA, 1983.
- C. Morris. *Foundations of the Theory of Signs*. University of Chicago Press, Chicago IL, USA, 1938.
- T. Muhr. Atlas.ti - the knowledge workbench, version 5.0. <http://www.atlasti.com>, 2004.
- W. Murray. Security should pay: It should not cost. In L. Yngström, editor, *Information Security - the Next Decade*, Amsterdam, Netherlands, 1995. International Federation for Information Processing, Kluwer Academic Publishers.
- S. Nachemson-Ekwall and B. Carlsson. *Guldregn: sagan om Skandia*. Bonnier fakta, Stockholm, 2004. Sophie Nachemson-Ekwall, Bengt Carlsson (Uddevalla: Mediaprint) 24 cm.
- NIST. *The Common Methodology for Information Technology Security Evaluation, CEM-97/017*. National Institute of Standards and Technology, Gaithersburg MD, USA, 1997.
- Organisation for Economic Co-operation and Development. *The revised OECD principles of corporate governance*. OECD, Paris, 2004.

- D. Parker. A new framework for information security to avoid information anarchy. In L. Yngström, editor, *Information Security - the Next Decade*, Amsterdam, Netherlands, 1995. International Federation for Information Processing, Kluwer Academic Publishers.
- D. Parker. The strategic values of information security in business. *Journal of Computers and Security*, 16:572–582, 1997.
- K. Popper. *The Open Society and Its Enemies*. Routledge, London, United Kingdom, 1945.
- PriceWaterhouseCoopers and DTI. Information security breaches survey 2004. Technical Report URN 04/617, PriceWaterhouseCoopers and Department of Trade and Industry, London, United Kingdom, 2004.
- S. Qing and J. Eloff, editors. *IFIP/SEC2000: Information Security - Information Security for Global Information Infrastructures*, Beijing, China, 2000. International Federation for Information Processing, International Academic Publishers.
- R. Rapoport. Three dilemmas in action research. *Human Relations*, 23 (4):499–513, 1970.
- Riksrevisionsverket. Datorrelaterade missbruk och brott - en kartläggning gjord av effektivitetsrevisionen. Technical report, Riksrevisionsverket, Stockholm, Sweden, 1997.
- H. Simon. *Administrative Behaviour*. Macmillan, New York NY, USA, 1948.
- M. Siponen. On the scientific background of information security management standards: a critique and an agenda for further development. In *Proceedings of the Second Annual Systems Security Engineering Conference (SSE)*, Orlando FL, USA, March 2001.
- SIS. *ISO 9000: svenska standarder för kvalitetsledning*. SIS (Standardiseringen i Sverige), Stockholm, 1997.

- SIS. Ledningssystem för informationssäkerhet, del 1: Riktlinjer för ledning av informationssäkerhet (swedish standard ss 62 77 99-1). Technical report, Swedish Standards Institute, Stockholm, Sweden, 1999a.
- SIS. Ledningssystem för informationssäkerhet, del 2: Specifikation för ledningssystem för informationssäkerhet (swedish standard ss 62 77 99-2). Technical report, Swedish Standards Institute, Stockholm, Sweden, 1999b.
- SIS. Ledningssystem för informationssäkerhet, del 1: Riktlinjer för ledning av informationssäkerhet (swedish standard ss-iso/iec 17799). Technical report, Swedish Standards Institute, Stockholm, Sweden, 2001.
- SSE-CMM Project. *Systems Security Engineering Capability Maturity Model. Model Description, Version 2.0*. SSE-CMM Project, Vienna VA, USA, 1999. <http://www.sse-cmm.org> accessed 2001-10-24.
- R. Stamper, K. Liu, M. Kolkman, P. Klarenberg, F. V. Slooten, Y. Ades, and C. V. Slooten. From database to normbase. *International Journal of Information Management*, 11:67–84, 1991.
- B. Starrin, L. Dahlgren, G. Larsson, and S. Styrborn. *Along the Path of Discovery: Qualitative Methods and Grounded Theory*. Studentlitteratur, Lund, Sweden, 1997.
- A. Strauss and J. Corbin. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Sage, Newbury Park CA, USA, 1990.
- G. Susman and R. Evered. An assessment of the scientific merits of action research. *Administrative Science Quarterly*, 23(4):582–603, 1978.
- M. Swartz and S. Watkins. *Power failure: the inside story of the collapse of Enron*. Doubleday, New York, 1st edition, 2003.

- Swedish Information Processing Society. Sba check product information and evaluation copy. <http://www.dfs.se/products/sbaeng/>, 2001a.
- Swedish Information Processing Society. Sba scenario method and program description. <http://www.dfs.se/products/sba/scenario/smetod.asp>, 2001b.
- United States. *The Sarbanes-Oxley Act of 2002: with analysis*. Lexis-Nexis/Matthew Bender, Newark, NJ, 2002.
- R. Von Solms. Information security management: Why standards are important. *Information Management and Computer Security*, 1(7), 1999.
- S. Von Solms. Information security - the third wave? *Journal of Computers and Security*, 19(7):615–620, 2000.
- M. Warren, S. Furnell, and P. Sanders. Odessa - a new approach to healthcare risk analysis. In L. Yngström and J. Carlsen, editors, *Information Security in Research and Business*, pages 391–402, London, United Kingdom, 1997. International Federation for Information Processing, Chapman & Hall.
- M. Wilson, D. Zafra, S. Picher, J. Tressler, , and J. Ippolito. *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. National Institute of Standards and Technology, Gaithersburg MD, USA, April 1998.
- L. Yngström. Education in safety systems and security analysis - suggestions for a one year university program. In *Proceedings of the IFIP TC11 first working conference on information security*. International Federation for Information Processing, 1983.
- L. Yngström. Experiences from a one-year academic programme in security informatics. In *Proceedings of the Fifth International Conference*

- on Computer and Security*. International Federation for Information Processing, 1988.
- L. Yngström. Experiences from a one-year academic programme in security informatics. *Information Age*, 11:77–82, 1989.
- L. Yngström. Security informatics 1985-1991: An assessment. Technical report, Department of Computer and Systems Sciences, Stockholm University and Royal Institute of Technology, 1991. SIIS-R-91.
- L. Yngström. Evaluation of an academic programme in it security 1985-1990. In *Computer Security: Discovering Tomorrow*. International Federation for Information Processing, 1993.
- L. Yngström. *A Systemic-Holistic Approach to Academic Programmes in IT Security*. PhD thesis, Stockholm University, Stockholm, Sweden, 1996.
- L. Yngström and F. Björck. The value and assessment of information security education and training. In L. Yngström and S. Fischer-Hübner, editors, *WISE 1, Proceedings of the IFIP TC11 WG 11.8 First World Conference on Information Security Education*, pages 271–292, Stockholm, Sweden, 1998. International Federation for Information Processing.

Ph.D. Theses

DEPARTMENT OF COMPUTER AND SYSTEMS SCIENCES

Stockholm University/KTH

www.dsv.su.se/eng/publikationer/index.html

Ph.D. theses:

-

No 91-004 **Olsson, Jan**

An Architecture for Diagnostic Reasoning Based on Causal Models

No 93-008 **Orci, Terttu**

Temporal Reasoning and Data Bases

No 93-009 **Eriksson, Lars-Henrik**

Finitary Partial Definitions and General Logic

No 93-010 **Johannesson, Paul**

Schema Integration Schema Translation, and Interoperability in Federated Information Systems

No 93-018 **Wangler, Benkt**

Contributions to Functional Requirements Modelling

No 93-019 **Boman, Magnus**

A Logical Specification for Federated Information Systems

No 93-024 **Rayner, Manny**

Abductive Equivalential Translation and its Application to Natural-Language Database Interfacing

No 93-025 **Idestam-Almquist, Peter**

Generalization of Clauses

No 93-026 **Aronsson, Martin**

GCLA: The Design, Use, and Implementation of a Program Development

No 93-029 **Boström, Henrik**

Explanation-Based Transformation of Logic programs

No 94-001 **Samuelsson, Christer**

Fast Natural Language Parsing Using Explanation-Based Learning

No 94-003 **Ekenberg, Love**

Decision Support in Numerically Imprecise Domains

No 94-004 **Kowalski, Stewart**

IT Insecurity: A Multi-disciplinary Inquiry

No 94-007 **Asker, Lars**

Partial Explanations as a Basis for Learning

No 94-009 **Kjellin, Harald**

A Method for Acquiring and Refining Knowledge in Weak Theory Domains

No 94-011 **Britts, Stefan**

Object Database Design

No 94-014 **Kilander, Fredrik**

Incremental Conceptual Clustering in an On-Line Application

No 95-019 **Song, Wei**

Schema Integration: - Principles, Methods and Applications

No 95-050 **Johansson, Anna-Lena**

Logic Program Synthesis Using Schema Instantiation in an Interactive Environment

No 95-054 **Stensmo, Magnus**

Adaptive Automated Diagnosis

No 96-004 **Wærn, Annika**

Recognising Human Plans: Issues for Plan Recognition in Human - Computer Interaction

No 96-006 **Orsvärn, Klas**

Knowledge Modelling with Libraries of Task Decomposition Methods

No 96-008 **Dalianis, Hercules**

Concise Natural Language Generation from Formal Specifications

No 96-009 **Holm, Peter**

On the Design and Usage of Information Technology and the Structuring of Communication and Work

No 96-018 **Höök, Kristina**

A Glass Box Approach to Adaptive Hypermedia

No 96-021 **Yngström, Louise**

A Systemic-Holistic Approach to Academic Programmes in IT Security

No 97-005 **Wohed, Rolf**

A Language for Enterprise and Information System Modelling

No 97-008 **Gambäck, Björn**

Processing Swedish Sentences: A Unification-Based Grammar and Some Applications

No 97-010 **Kapidzic Cicovic, Nada**

Extended Certificate Management System: Design and Protocols

No 97-011 **Danielson, Mats**

Computational Decision Analysis

No 97-012 **Wijkman, Pierre**

Contributions to Evolutionary Computation

No 97-017 **Zhang, Ying**

Multi-Temporal Database Management with a Visual Query Interface

No 98-001 **Essler, Ulf**

Analyzing Groupware Adoption: A Framework and Three Case Studies in Lotus Notes Deployment

No 98-008 **Koistinen, Jari**

Contributions in Distributed Object Systems Engineering

No 99-009 **Hakkarainen, Sari**

Dynamic Aspects and Semantic Enrichment in Schema Comparison

No 99-015 **Magnusson, Christer**

Hedging Shareholder Value in an IT dependent Business society - the Framework BRITS

No 00-004 **Verhagen, Henricus**

Norm Autonomous Agents

No 00-006 **Wohed, Petia**

Schema Quality, Schema Enrichment, and Reuse in Information Systems Analysis

No 01-001 **Hökenhammar, Peter**

Integrerad Beställningsprocess vid Datasystemutveckling

No 01-008 **von Schéele, Fabian**

Controlling Time and Communication in Service Economy

No 01-015 **Kajko-Mattsson, Mira**

Corrective Maintenance Maturity Model: Problem Management

No 01-019 **Stirna, Janis**

The Influence of Intentional and Situational Factors on Enterprise Modelling Tool Acquisition in Organisations

No 01-020 **Persson, Anne**

Enterprise Modelling in Practice: Situational Factors and their Influence on Adopting a Participative Approach

No 02-003 **Sneiders, Eriks**

Automated Question Answering: Template-Based Approach

No 02-005 **Eineborg, Martin**

Inductive Logic Programming for Part-of-Speech Tagging

No 02-006 **Bider, Ilia**

State-Oriented Business Process Modelling: Principles, Theory and Practice

No 02-007 **Malmberg, Åke**

Notations Supporting Knowledge Acquisition from Multiple Sources

No 02-012 **Männikkö-Barbutiu, Sirkku**

SENIOR CYBORGS- About Appropriation of Personal Computers Among Some Swedish Elderly People

No 02-028 **Brash, Danny**

Reuse in Information Systems Development: A Qualitative Inquiry

No 03-001 **Svensson, Martin**

Designing, Defining and Evaluating Social Navigation

No 03-002 **Espinoza, Fredrik**

Individual Service Provisioning

No 03-004 **Eriksson-Granskog, Agneta**

General Metarules for Interactive Modular Construction of Natural Deduction Proofs

No 03-005 **De Zoysa, T. Nandika Kasun**

A Model of Security Architecture for Multi-Party Transactions

No 03-008 **Tholander, Jakob**

Constructing to Learn, Learning to Construct - Studies on Computational Tools for Learning

No 03-009 **Karlgren, Klas**

Mastering the Use of Gobbledygook - Studies on the Development of Expertise Through Exposure to Experienced Practitioners' Deliberation on Authentic Problems

No 03-014 **Kjellman, Arne**

Constructive Systems Science - The Only Remaining Alternative?

No 03-015 **Rydberg Fåhræus, Eva**

A Triple Helix of Learning Processes - How to cultivate learning, communication and collaboration among distance-education learners

No 03-016 **Zemke, Stefan**

Data Mining for Prediction - Financial Series Case

No 04-002 **Hulth, Anette**

Combining Machine Learning and Natural Language Processing for Automatic Keyword Extraction

No 04-011 **Jayaweera, Prasad M.**

A Unified Framework for e-Commerce Systems Development: Business Process Patterns Perspective

No 04-013 **Söderström, Eva**

B2B Standards Implementation: Issues and Solutions

No 04-014 **Backlund, Per**

Development Process Knowledge Transfer through Method Adaptation, Implementation, and Use

No 05-003 **Davies, Guy**

Mapping and Integration of Schema Representations of Component Specifications

No 05-004 **Jansson, Eva**

Working Together when Being Apart – An Analysis of Distributed Collaborative Work through ICT from an Organizational and Psychosocial Perspective

No 05-007 **Cöster, Rickard**

Algorithms and Representations for Personalised Information Access

No 05-009 **Ciobanu Morogan, Matei**

Security System for Ad-hoc Wireless Networks based on Generic Secure Objects