KUNGL
TEKNISKA
HÖGSKOLAN

HØGSKOLEN
I GJØVIK

NISlab
Norwegian Information
Security Laboratory

Key factors in making Information Security Policies Effective

Gullik Wold

Institutionen för
Data- och Systemvetenskap

Examensarbete
Nr 2004-x-164
2004

Examensarbete 20 poäng
i data- och systemvetenskap
inom magisterprogrammet i informations- och kommunikations säkerhet,
Kungl Tekniska Högskolan

Master's Thesis

Name of candidate:	Gullik Wold
Title of paper:	Key factors in making Information Security Policies Effective
Line:	02HMAISA
Branch of study:	Masters Program
Sphere:	Information Security
Period:	01.01.2004 -30.06.2004
Email:	gullik.wold@ergo.no
Version:	27.09.2004

To Andreas and Bjørnar.

The natural thirst that is never quenched is the thirst for knowledge
-Dante Aligheri

Abstract

The aim of this work is to reveal key factors that characterize an effective information security policy. The challenge has been to find out what not knowing and not understanding in the search for factors that makes a security policy effective, and to design a questionnaire good enough to obtain and distinguish the key factors of interest.

The survey approached “large” organizations in which information- and communication technology (ICT) is considered being an essential part of the daily operation.

The postal questionnaire, revealed considerable differences between organizations reporting “high” and “low” values on “effect” of the security policy and “organizational security robustness". Respondents reporting high values perform significantly better on the “human oriented” parameters that appear to be key factors:

- Engagement from management
- Learning/awareness
- Cultural aspects (behaviour and attitude)
- Personal bonding
- Measuring, reporting, following up
- Focus attainable security objectives involving the working processes

All work concludes that the human side of enterprise is important. It is crucial to the effectiveness and success of the security work that the security policy describes attainable security objectives involving the working processes.

It is a common agreement among the respondents that most of the security breaches can be looked upon as unintended incidents perceived as faults and accidents caused by human error. This assumption is important to be aware of related to the work with the security policy and its most pronounced causes to security breaches.

Organizations that perform “measurement, reporting and following up” on either organization level, or related to security policies gain higher scores on “effect”. The results indicate that monitoring and measuring the environment in question leads to a higher level of focus and control.

The implementation of effective security controls is dependent upon creating a security positive environment where employees understand and engage in the behaviour that is expected of them. The use of security awareness to create and maintain security positive behaviour is a critical element in achieving this.

All results supports that “engagement from management” is an important factor in achieving appropriate conditions in the aim of making security policies effective.

Sammendrag

Målet med denne oppgaven har vært å finne frem til nøkkelfaktorer som kjennetegner en effektiv policy for informasjonssikkerhet. Utfordringen har vært å finne frem til hva vi ikke vet og ikke forstår i arbeidet med å finne frem til faktorer som gjør en policy effektiv, og samtidig lage en undersøkelse god nok til å frembringe og skille ut nøkkelfaktorer av betydning.

Undersøkelsen henvendte seg til ”store” virksomheter hvor informasjons- og kommunikasjons teknologi ble ansett å utgjøre en vesentlig del av den daglige aktiviteten.

Fra spørreundersøkelsen ble det funnet store forskjeller hos virksomhetene som rapporterte ”høye” og ”lave” verdier på ”effekt” av sikkerhetspolicyen og ”virksomhetens sikkerhetsmessige robusthet”. Respondentene som rapporterer høye verdier yter betydelig bedre på parametrene ”personrelaterte forhold” som gir følgende nøkkelfaktorer:

- Engasjement fra ledelsen
- Læring /”awareness”
- Holdninger
- Samhandling
- Måling, rapportering, oppfølging
- Fokus på sikkerhetsmål som involverer arbeidsprosessene

Alt arbeid konkluderer med at fokus på de menneskelige faktorer er viktig. For å oppnå effektivitet og suksess i sikkerhetsarbeidet er det avgjørende at sikkerhetspolicyen beskriver oppnålige sikkerhetsmål som involverer arbeidsprosessene.

Det er en felles oppfatning blant de som har besvart undersøkelsen at de fleste sikkerhetsbrudd kan betraktes som ikke tilsiktede hendelser som kan oppfattes som feil og uhell forårsaket av mennesker. Dette er et forhold det er det viktig å være oppmerksom på i arbeidet med sikkerhetspolicyen og dens mest uttalte årsaker til sikkerhetshendelser.

Virksomheter som utfører ”måling, rapportering og oppfølging” enten på virksomhetsnivå eller av sikkerhetspolicyen oppnår bedre resultater på ”effekt”. Resultatene indikerer at overvåkning og måling av det aktuelle miljøet fører til høyere nivå med hensyn på fokus og kontroll.

Effektive sikkerhetsmekanismer er avhengig av et sikkerhetsbevisst miljø hvor de ansatte forstår nødvendigheten og samtidig engasjerer seg i sikkerhetsarbeidet. Bruk av bevissthetstrening for å oppnå og vedlikeholde et sikkerhetsfremmende miljø er et avgjørende element for å oppnå dette.

Alle resultater understøtter at “engasjement fra ledelse” er en viktig faktor for å tilrettelegge forholdene med hensyn på målsettingen å oppnå en effektiv sikkerhetspolicy.

Preface

This Master' thesis is written in partial fulfilment of the requirements for the degree of Master of Science in Information security at Gjøvik University College. The thesis has been under work during the period 1.1.-30.06.2004.

Defining the scope of work was a student objective. The reason for my choice in approaching work with Information security policies is the curiosity about the vision and mission of this document and which role it may play in achieving adequate security.

During my experience within the security field, it has often been recognized that the documents existence is normally known, but its appearances rarely seen. Many templates have been looked upon, some thick some thin. The knowledge and sense of the documents mission and what effect that could be expected from its use has to me been somewhat diffuse. It has been my intention to write a paper in the aim to clarify these aspects hence reveal the "key factors" decisive.

In an article of Lara Wills, Security Policy Effectiveness [Wills 2002] *p.11* she is discussing the importness regarding measurement. "What good is a policy if you don't take the time to measure its effectiveness?

The work with the thesis project plan [Wold 2003] also revealed a need for measurement and proposed a pilot metrics program.

Being in the fortunate situation that a colleague in ErgoIntegration AS approached a corresponding thesis work, the possibility to gain a mutual effect looked very interesting and ended up in following. Geir Simonsen in his MSc. thesis "En prosess for sikkerhetsmetrikk program" carries out a measuring approach (A process for security metrics programs) [Simonsen 2004]. The thesis includes a toolkit, which is assessed used in a pilot in our company ErgoIntegration AS.

A part of the pilot is indented based on the findings and key factors found in this thesis making an information security policy effective. The purpose in accomplishing a pilot related to "security metrics program" is to find out in to what extent meaningful results are produced and achieved, and to what extent uses of security metrics prove substantive justifications for decisions stated in an implemented security policy.

The work has been very interesting and I gained a lot of knowledge about policies and security that for sure will improve my further work within the field of information security.

Lørenskog 30th June 2004

____

Gullik Wold

Acknowledgements

Thank you to teaching supervisor Prof. Einar Snekkenes for useful feedback during the work.

Thank you to Prof. Louise Yngström and her colleagues at Department of Computer and Systems Sciences, Stockholm University for the impressive hostage during our visit in March. The effort you put into the program contributed to the valuable experience to all of us, gaining useful insight in your sphere and in addition responding valuable comments to our works. Also thank you to my opponent Arne Roar Nygård for useful comments

Thank you also to my employer ErgoIntegration AS for the possibility to fulfil this study during these two years.

Thank you to Gro, Andreas and Bjørnar for your patience in my absence of writing.

Summary of contributions

The thesis includes a survey with use of a postal questionnaire. In the initial phase of the work, it was planned for an arrangement in approaching the Security Officer (SO) and a number of employees in each organization. Pilot was carried out in one of the companies within ErgoGroup, which uncovered the challenge in this way of gathering information. It was then concluded to reduce the limit of extent to only approach the Security Officer. Thank your for help and assistance in the work with the pilots to Jan Erik Lilleng, Viggo Hansen and Eirik Pettersen in ErgoIntegration AS and Knut Assev in ErgoEphorma AS. Jan Erik's lead in use of the Excel workbook[1] from company VincIT AS was of vital importance in conducting the questionnaire. Hints from Ole Kristian Målbakken in VincIT eased the work in utilizing the program core.

Thank you to all of you who took the time and effort in answering the questionnaire. It was of great help and hopefully, it has contributed to reveal some knowledge of interest.

Thank you to all of you receiving the questionnaire. It contributed to gain anonymity of the survey.

Quality and limitations of this work

In writing, it was chosen to extend the definition security policy from Information and Communication Technology (ICT) security policy to Information security policy due to its superior role as a management level document. The definition and use of the notion Information security and IT security however varies. Information security is in some literature defined to embrace both administrative (procedural) security[2] and IT security. IT security is defined as ADP (computer security) and communications security.

[1] "Bekymringsorientert risikovurdering program"

[2] Security mainly obtained by means of administrative rules and procedures which also deal with written and spoken information.

The need for policies and their framework will in to some extent vary depending on the size of the organization in question. This work is aimed at large organizations with more than 100 employees.

Outline of the thesis

The thesis is outlined in eight chapters. Three chapters embrace the main research the “State of the art”, “The Survey” and the “Analysis”. The “State of the art” is based on a survey for information exploring scientifical databases, relevant books and educational papers. The “Survey” part is based on a postal questionnaire designed upon findings from the literature survey. The “Analysis” part is based on the findings from both literature and questionnaire surveys.

Each part is finalized with a summary. The chapter “Conclusion” summarise all findings in to a conclusion.

Audience

The thesis focuses on a superior corporate document and is of main interest for personell responsible for management and security within the organisation.

Abbreviations

SP - security policy
SO - security officer

Table of content

List of Figures

List of Tabels

1 SECURITY BY POLICY

1.1 Security by policy

It is not the strongest of the species that survive, nor the most intelligent. It is the one most adaptable to change-

- Charles Darwin

1.2 Introduction

The information security policy is an important control needed within an organization to manage the implementation and ensure the effectiveness of information security.

The information security policy is essentially the direction-giving document in an organization and defines the broad boundaries of information security. Furthermore, it indicates management's commitment to, and support for, information security in an organization and defines the role it has to play in reaching and supporting the organization's vision and mission.

Documenting an information security policy that reflects the organization's vision and mission and at the same time entrenching the policy in the organization so that it becomes a normal and acceptable part of day-to-day operations is difficult at best.

Quite often, users are ignorant of the policy's existence; users do not fully understand the document; it is too long or too technical; users do not see the relationship between the policy and their daily tasks and see it as a nuisance. Unfortunately, a common problem with most information security policies is that they fail to impact the users 'on the ground'. [Höne, Eloff 1/2002] *p.1*

1.3 Justification for the research

In reference to Höne and Eloff - to obtain good security the organization must maintain ability to handle threats with protective measures in an adequate way. To be able to handle the challenge a strategy is needed which must be outlined in adequate documentation or policies. The security policy is one of the most important controls needed within an organization to manage the implementation and ensure the effectiveness of information security.

What is the right level of control such that risk is mitigated and security supports business objectives? That is the essence of IT security governance and the responsibility of the security officer. Too much governance and you inhibit innovation and the ability to react quickly to new opportunities. Too little governance and you expose the business to unnecessary risks. The balance needs to be just right. [Brooke 2004] *p.1*

Even this point of view is adequate seen from a business view; is it important not to forget the fact that most of the larger organizations are set under jurisdiction of official law and regulations which rarely are subject for discussion.

Due to the complexity and to that Information Communication Technology (ICT) security embraces most of the organization is it of interest to find out if there are any factors that are more pronounced in achieving good effect in accomplishment of a security policy.

Most parties as stakeholders, management, security officers, customers, users etc. should gain interest of how organizations approach implementation of security policies and what effect and experience is revealed during accomplishment.

1.4 Research idea

Literature indicates that there is a reason to believe that a majority of security breaches happens related to improper and imperfect behaviour due to the security policies in place which in turn led us into the research question:

- *What factors are essential in making an information security policy effective?*

1.5 Research problem

A research problem is motivated not by palpable unhappiness, but by incomplete knowledge or flawed understanding. You solve it not by changing the world but understanding it better. Practical and research problems have the same structure, but their conditions and costs differ in important ways:

The condition of a practical problem can be any state of affairs whose cost makes you (or someone) unhappy. The condition of a research problem, on the other hand, is always some version of not knowing or not understanding something. [Booth, Colomb, Williams 2003] *p.59-62*

In accordance with the statement above a less effective security policy most likely is a vast of resources and worse, lack of ability in preventing security breaches.

In the aim of verifying which factors that gain effect in making the security policy effective this must be looked upon as a matter of not knowing or not understanding something, and thus leads us into research.

The performance of IT security is difficult to manage without being measured. A way to obtain this is use of metrics. Because IT governance is about alignment with business objectives, metrics should be developed and reported within a business context. Without measuring, you are flying blind. [Brooke 2004] *p.1*

1.6 Research approach

In the nature of the fact that the course of action in compiling a security policy will depend on many factors and largely will vary from organization to organization, it induces that an answer covering all questions is not likely to be found. However, the method chosen must be able to reveal (fundamental) general problems (facts).

The intention has been to find out what not knowing and not understanding in the search for factors that makes a security policy effective. The challenge is to find research papers related to the topic and to design a questionnaire in a way that answers the questions of not knowing and not understanding the causes to effectiveness.

The thesis preliminary work with the project-plan evaluated whether security metrics could be expedient to measure performance of an implemented security policy. Three areas appeared essential to measure, human, technical and economy factors. It was not evaluated in to what extent the policy itself (design, outline, how communicated) or its surroundings due to these three factors was decisive due to effectiveness.

The apprehension is that a quantitative method is preferable in the aim to reveal behaviour and attitudes within a defined search area. The search area was decided upon findings from “State of the art”.

Quantitative research seeks to develop relevant true statements, ones that can serve to explain the situation of concern or that describe the causal relationships of interest. In quantitative studies, researches advance the relationship among variables and pose this in terms of questions or hypotheses. [Creswell 2003] *p.8*

In reference to Creswell on *p.14*, a reasonable strategy in exploring this problem is by use of a survey approach. The researcher brings to the choice of a research design, assumptions about knowledge claims. Surveys include cross-sectional and longitudinal studies using questionnaires or structured interviews for data collection, with the intent of generalizing from a sample to a population.

The research approach is with project plan in mind to look at existing literature hence to gain knowledge about how professionals and security standards approach the superior policy issue.

From that, the challenge and further work will be to design a questionnaire good enough to obtain and distinguish the key factors of interest. The research will approach large organizations in which ICT is an essential part of the activity. However, even in the anticipation of that the respondents emphasize adequate security we assume an extent of heterogeneousity.

The purpose is that the survey should be good enough to:

– *develop relevant true statements, ones that can serve to explain the situation of concern or that describes the casual relationships of interest.*

One of the most important aims with the survey will be to achieve a common understanding of the challenges in such a research.

2 STATE OF THE ART

To identify and find out which factors are essential in achieving effective Information security policies we have to get hold of what knowledge is present for this area preferably from a holistic vision.

> “Holistic vision is really quite simple – it is the ability to look at a business problem or opportunity from many different angles simultaneously, and over different time scales.” [Grundy 1995] *p.1*

In addition, it is of interest to find out to what extent, this knowledge is based on theories or verified knowledge from practical experiments.

To accomplish this, a survey of information has to be done. The survey will start by searching in what is considered reliable scientific databases and in environments known for experience and professionalism in this area.

The aim of the survey is to look for and identify present knowledge embracing reflections, considerations, problems, statements, etc. related to the policy and which is considered to be of interest to have in mind when formulating the questionnaire.

The “Findings” are listed for each chapter and summarised at the end of State of the art. The list is most likely not exhaustive, but it is a start and it will be easy for the community to include new elements found for later use.

2.1 The security policy - where to start

Policies can be designed for whatever level or operation needed and when the definition security policy is used, it can be difficult to recognize to which type of security policy we are talking about. In our work, we are focusing on the superior or top-level information security policy.

2.1.1 Why does security need a policy

Why do security issues need policies, which in reference to Webster are a definite course of action? From IETF [RFC 2196] *p.6* “What is a Security policy and why have one”? Following argument is pointed out:

> “The security-related decisions you make, or fail to make, as administrator largely determines how secure or insecure your network is, how much functionality your network offers, and how easy your network is to use. However, you cannot make good decisions about security without first determining what your security goals are. Until you determine what your security goals are, you cannot make effective use of any collection of security tools because you simply will not know what to check for and what restrictions to impose.”

Looking at the strategy for corporate matters:

> "Strategy is about getting from where you are now to a place where it is worthwhile being. Strategy is also about getting there trough competitive advantage, with least difficulty and in least time". [Grundy 1995] *p.11*

The Paper "A Framework for Information Security Culture" Could it Help on Solving the Insider Problem? [Kufås 2002] *p.12* holds up following definition on security:

> "Security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of disturbance or injury …security holds a mirror up, not to nature, but to society and its institutions".

Holding these two definitions up to each other major differences unveil.

– Corporate strategy is about reaching a goal with least difficulty and in least time.

– Security is responsible for that the goal is met without disruption or harm and without fear of disturbance or injury.

In "Using security metrics to assess risk management capabilities" [Kormos & et.al 1999] *p.10* a figure shown in the paper is of interest in understanding the different objectives discussed related to cooperation and security.

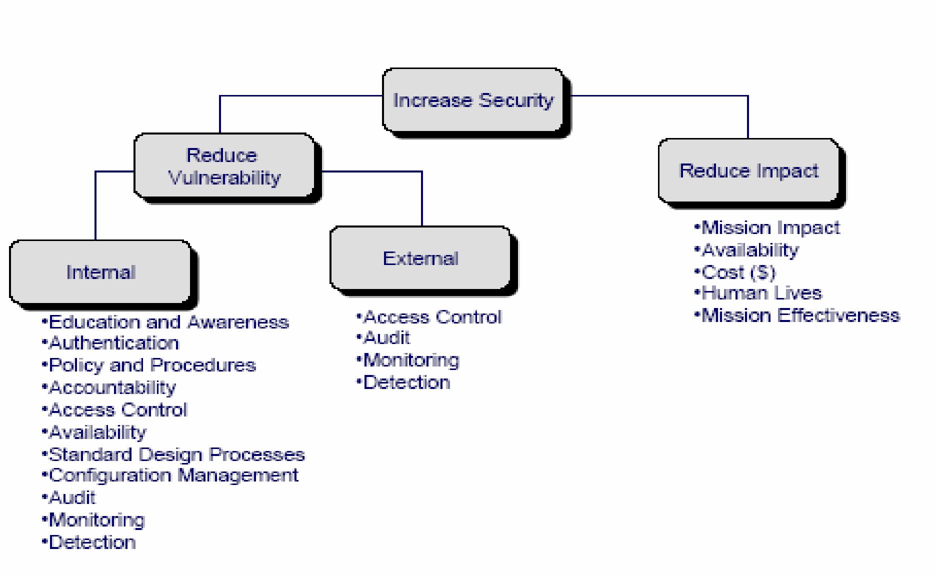


Figure 2-1. Illustrating difference between corporate and security objectives

The top-down approach illustrated in Figure 2-1 [Kormos & et.al 1999] *p.10* considers the guidance and policy and the user, security professional, auditor, and management perspectives.

> "Security professionals and auditors often focus on reducing threats and vulnerabilities to increase security, whereas users and managers focus on operational capability, low cost, and user friendliness.
>
> Managers are seeking a return on investment and therefore tend to focus on factors that reduce negative effect on their mission, total costs, and human life."

It is easily seen that security is a question of balancing resources used in protecting assets from threats. It is easy to understand that handling the entire spectre of security issues in a balanced way is an embracing task that requires a high degree of awareness and control in being effective. An accepted management principle is that an activity cannot be managed if it cannot be measured. Security falls under this headline.

To manage an organization strategy and within the business objectives is of course the challenge most organizations and their teams face daily. Many issues within the framework of political factors, economic factors, social factors and technological factors have to be taken into consideration in an effective way.

To handle all these elements without a policy stating the goals and objectives would be an impossible task.

The technological factor is of course important, but is only a part of the total framework within the business objectives of the organization. Its important not to forget that the purpose of information technology and hence information security plays a supportive role in achieving the organization's daily business objectives and long-term strategy.

Within the security framework, the information security policy is one of the most important controls needed within an organization to manage the implementation and ensure the quality and effectiveness of information technology.

Findings from Chapter 1
Finding 2-1. User don't see relationship between security policy and daily tasks
Finding 2-2. Users often lack knowledge of the security policy's existence
Finding 2-3. Security policy often seems to be ineffective
Finding 2-4. Security policy is often looked upon as a nuisance – lack of respect

Findings from Chapter 2.1
Finding 2-5. Determine what your security goals are (know your assets and their threats)
Finding 2-6. Security policy shall balance corporate interests and security measures
Finding 2-7. Security cannot be managed if not measured.
Finding 2-8. Security policy is one of the most important controls in management of security

2.2 How professionals define security policy

The notions security and policy is as mentioned two all embracing words and an exact or precise definition is hardly expected to be found. Webster defines policy as:

> "A definite course of action adopted for the sake of expediency, facility or the like".

Literature and articles offer different explanation and definitions. In the aim of getting a firm footing on the subject, it should be appropriate to look at the professionals and their definition of what this document ought to be.

Bundesamt für Sicherheit in der informationstechnic BSI [BSI 2003] *(S 2.192)*

> "The Information Security Policy defines the level of IT security to which the organisation aspires. The Information Security Policy contains the IT security objectives which the organisation has set itself and the IT security strategy it pursues."

The Critical Infrastructure Assurance Office (CIAO) [CIAO 2000] *p.3* defines an Information Security Policy as:

> "Set of rules and practices an agency uses to manage, protect, and allocate its information resources".

The Department of trade and industry, UK [DTI 2003] *p.2*

> "A corporate policy sets out an organisation's intentions and principles regarding information security. It should be timeless in that it should alter little from year to year. Corporate policy must: be clear and unambiguous, include statements covering:
>
> – scope
> – legal and regulatory obligations
> – roles and responsibilities
> – strategic approach and principles
> – approach to risk management
> – action in the event of a policy breach."

Government Communication HQ/Communications-Electronics Security Group (GCHQ/CESG) [CESG 2002] *p.4*

> "All organisations need to protect their information by adopting appropriate security measures. These can be organisational, physical, technical or educational. Such measures must be based on a coherent security policy. This policy must be derived from a sound assessment of the threat to an organisation's information and the impact of corruption or loss of that information. Advice on constructing and implementing a security policy is available in the Code of Practice for Information Security Management, BS7799, and in the DTI's Information Security Assurance Guidelines for the Commercial sector".

IETF Network Working Group, RFC: 2196 [RFC 2196] *p.6*, Definition of a Security Policy

> "A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."

Information Security Forum [ISF 2003] *(Section SM1.2)*

> "Objective: To document top management's direction on and commitment to information security, and communicate it to all relevant individuals.
>
> Principle: A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the enterprise's information and systems."

National Institute of Standards and Technology (NIST) [NIST 800-14] *p.13* notes in Special Publication 800-14, Guide for Developing Security Plans for Information Technology Systems:

> 3.1 Policy
>
> "The term computer security policy has more than one meaning. Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term policy is also used to refer to the specific security rules for particular systems. Additionally, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization's e-mail privacy policy or fax security policy."

The New South Wales Department of Commerce, Australia [NSW 1/2003] *p.7*, gives a description in Information Security Guideline for NSW Government – Part 3, Information Security Baseline Controls, Current version: June 2003,

> 3.1 Information Security Policy
> Information security is a responsibility shared by all members of the agency, which needs to be led by clear and visible management policy and procedures.
>
> A policy issued and approved by executive management should clearly define the agency's direction on Information Security, including the use of assets, the performance standards expected and the conduct of all users within the agency.
>
> The agency's policy must be clearly communicated to and acknowledged by all personnel.
>
> Effective policy and procedures, backed by management commitment are an important front line defence against information security breaches. Reliance cannot be placed on technological measures alone.
>
> Procedures, guidelines and standards for the performance of business and administrative functions, in support of the information security policy, should be developed. These procedures should be kept current and clearly communicated to all personnel.

It is no problem to prolong the list of approaches to what a security policy is or ought to be.

The above list is of course not exhaustive and only a flash of complete documents and does not offer the complete story.

However, it is not easy from the definitions referred or reading the complete documents to understand what a security policy is really about and what results are expected from it.

2.3 Evaluation of international information security standards

The security policy this vital direction-giving document is, however, not always easy to develop and the authors thereof battle with questions such as what constitutes a policy. To compensate "lack of knowledge" the policy authors turns to existing sources for guidance. One of these sources is the various international information security standards.

The paper [Höne, Eloff 2/2002] evaluates the current Information security standards. The standards recognize that the information security policy is an important topic and therefore it is generally covered early on in the different standard documents.

Each of the international information security standards described was measured against the list of elements and general characteristics[3] of an information security policy to determine its coverage in the various standards.

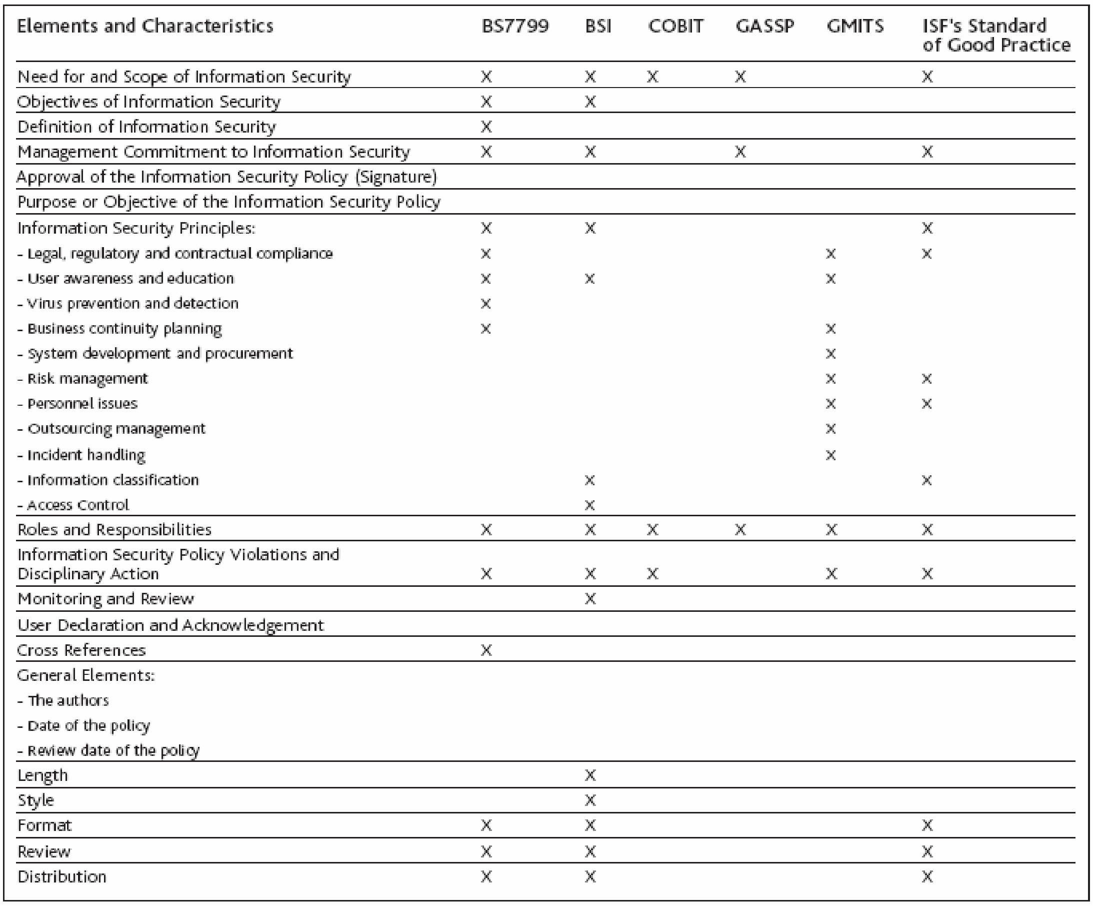
[3] The elements and characteristics are enclosed in the appendices.

The paper is of interest in the way that it describes a set of elements that is considered important in the aim of achieving a complete and adequate security policy. The elements focus mainly on the overall content of the policy.

The extent to which the policy as a topic is covered in these documents, however, differs vastly, with some of them spending only one or two short paragraphs on the topic, and others provides concise point-by-point guidance.[4] [Höne, Eloff 2/2002] *p.406*

The standards constitutes a framework or cookbooks in understanding business information security requirements, the need to establish policy and objectives for information security; implementing and operating controls in the context of managing an organization's overall business risk.

The table below gives an indication of which elements and characteristics were indeed covered in the standards (indicated by the X marks in the various columns). It should, however, be noted that the table does not give any indication of the extent of the coverage, i.e. whether the elements or characteristics are simply mentioned or whether they are in fact explained in detail.



Elements and Characteristics	BS7799	BSI	COBIT	GASSP	GMITS	ISF's Standard of Good Practice
Need for and Scope of Information Security	X	X	X	X		X
Objectives of Information Security	X	X				
Definition of Information Security	X					
Management Commitment to Information Security	X	X		X		X
Approval of the Information Security Policy (Signature)						
Purpose or Objective of the Information Security Policy						
Information Security Principles:	X	X				X
- Legal, regulatory and contractual compliance	X				X	X
- User awareness and education	X	X			X	
- Virus prevention and detection	X					
- Business continuity planning	X				X	
- System development and procurement					X	
- Risk management					X	X
- Personnel issues					X	X
- Outsourcing management					X	
- Incident handling					X	
- Information classification		X				X
- Access Control		X				
Roles and Responsibilities	X	X	X	X	X	X
Information Security Policy Violations and Disciplinary Action	X	X	X		X	X
Monitoring and Review		X				
User Declaration and Acknowledgement						
Cross References	X					
General Elements:						
- The authors						
- Date of the policy						
- Review date of the policy						
Length		X				
Style		X				
Format	X	X				X
Review	X	X				X
Distribution	X	X				X

Table 2-1. Policy elements and characteristics covered in the standards

[4] All the international standards researched are available in the public domain in various formats.

Höne and Eloff conclude that the international standards, however, are not comprehensive in their discussions of the Information security policy, with some of them covering the topic in one or two short paragraphs only. These standards attempt to describe the various processes and controls needed for successfully implementing an Information security policy, rather than advising what the policy should look like.

In our work in finding factors related to effectiveness, two of the elements are decided to be of particular interest in our further examination.

> **"Management Commitment to Information Security"**
> The commitment statement is the singularly most important statement in an information security policy. Without this statement, any activities attempted by the information security personnel will not be effective and will not be taken seriously throughout the entire organisation. The management commitment statement can force employees to pay attention to information security and demonstrates management's intention of making a success of it in the organisation."
>
> **"Monitoring and Review"**
> This statement deals with the need to frequently monitor and review the continued applicability and effectiveness of the information security controls implemented within the organisation. Without this statement there is no forced continuity for the improvement of information security implementation in the organisation."

It is also of interest to notice that the international security standards are not necessarily comprehensive in the guidance of how to write and implement a security policy.

However Frank-Arne Stamland in his MSc thesis "Is BS7799 worth the effort" [Stamland 2004] *p.51* concludes that:

> "organisations that use the standard informally have higher maturity than those organisations that do not implement any ISMS."

Use of standards, seems to gain value about the security challenges and knowledge about the organization strengths and weaknesses and as such a support in the work in writing an adequate policy.

In guideline "Information Security Guideline for New South Wales Government" [NSW 2/2003] *p.17* states that:

> "Executive management should set a clear direction and demonstrate their support for and commitment to the Information Security Management System (ISMS) by issuing a formally agreed and documented ISMS policy across the agency. The policy should be endorsed and signed by the Chief Executive Officer."

The security policy is the primary management document in maintaining the security strategy and objectives. The security policy is to be compared with the corporate policy in describing the goals and objectives.

Findings from Chapter 2.3
Finding 2-9. Management commitment to information security is most important
Finding 2-10. Monitoring and review is an important element
Finding 2-11. International standards are not comprehensive in their discussions of security policy

2.4 Why security policies fail

In an article of Rosemary Sumajit [Sumajit 2002] *p.1*, she is wording that Security is a myth and that we are talking about managing a risk based on following discussion.

> "There is a great big myth about security. People believe that it exists. According to the Merriam-Webster Collegiate Dictionary, security literally means 'freedom from danger'. But danger exists everywhere, so this is simply not possible. Even though we may use the word security, we are really talking about taking measures that will reduce the likelihood of danger or mitigate the effects of a breach.

James P. Cavanagh [Cavanagh 2002] *p.3* discuss the classic 'citadel' model which has been a common way to look upon security and states that security is more a risk analysis exercise.

In a work conducted by Department of Industrial Economics and Technology Management Norwegian University of Science and Technology & NSM – Nasjonal sikkerhetsmyndighet about "Information security and the Insider problem"[ROSS 2003] a report including five papers discuss issues due to area of problems regarding human and organizational factors related to information security.

From the Paper II written in the context of the project: Information security and the Insider problem, "The Human Factor" [Mølmann 2003] *p.3* refers to following history:

> "History tells of an incident from the late 1200s, where Kublai Khan and his Mongol hordes tried to go through, go under and go around the Great Wall of China, but the wall was too solid, too deep and too long. Still, he finally managed to conquer the obstacle – and most of China – by simply bribing the gatekeeper. The morale is that no matter how strong presence of technical control, the security always depends on the people within the organization. The human factor should thus not be ignored".

These quotations draw a good picture of what security is about:

- Freedom from danger by managing risk were use of technical means and human factors plays a vital role.

At the same time the policy shall be entrenched in the organization so that it becomes a normal and acceptable part of day-to-day operations in an effective way. [Höne, Eloff 2/2002] *p.1*

A white paper from Control Data "Why Security Policies Fail" [Control Data 1999] *p.4* [5] discussing "natural weaknesses" and "real" threats of security policies commonly overlooked.

In examination of the "natural weaknesses", it has emphasized that before attempting to develop a security policy one must acknowledge certain weaknesses in the processes of securing any asset.

- Security is a barrier to progress.

> "Even common sense security measures reduce productivity. "Protection" is annoying, wastes time, and pushes the patience limit. Red light is passed under the assumption that light was broken or that waiting time was unacceptable."

[5] The report seems to be the most thorough work accessible and is often cited.

The report "A Framework for Information Security Culture" [Kufås 2002] *p.3* focuses on that Security is a learned behaviour and that self-preservation is instinctual behaviour.[6] Securing assets is about protecting from deliberate actions and is a higher-level function that must be learned and occasionally reinforced.

> "The field of human behaviour according to the use of computers and information handling is complex due to the many different types of actions. Computer misuse can be the result of external pressure, psychological state or lack of competence. Omission or commission of the rules or policy of an enterprise can be realized knowingly or unknowingly and intentionally or unintentionally. This raises the question of what we actually are protecting us from. Traditionally, there exist a distinction between the terms security and safety, where safety means protection from accidental incidents, and security is about deliberate actions"

In an article by Charles Cresson Wood [Wood 2000] *p.2* "An unappreciated reason why information security fails" he is arguing that it cant be expected that users are to repeatedly look at a centralized information security policy, and hence bound to lead to disappointing results.

> "This due to the fact awareness programmes tries to sensitize people to the fact that there are many information security issues that they need to worry about e.g. in trying to get people to use policies, procedures, standards, architectures, and other requirements. Yet massive levels on none compliance prevail at many organizations".

Human error rather than flawed technology is the root cause of most security breaches. Therefore, the challenge for many organizations is to create a security-aware culture.

- Making staff aware of the risks and their responsibilities helps them act in as sensible and secure manner. [ISBS 2004] *p.8*

The "real" threats are often from within:

- The real threat to information assets is non-malicious damage resulting from human error, denial of service, and inappropriate disclosure. [Control Data 1999] *p.5*

Security is a learned behaviour.

- If a user is unaware of the value of a particular policy, they will believe the policy is stupid and therefore, not follow it. [Control Data 1999] *p.4*

In reference to the paper "Security Scandinavian style", [Björck 2001] *p.5-6* discusses the issues related to culture and human factors in security.[7]

> "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".

From the citations, we understand that the reason why security policies fail is due to several reasons made up of many factors related to the embracing definition of security, which include

[6] We can draw a parallel to definition of safety, which at its simplest means protection from accidents.

[7] By modelling the ISMS process – a software tool was developed against which organisations attempting to attain, a management system for information security can benchmark their current practices.

human, technical and economical factors. Making a security policy that supports security effectiveness, it is essential to pose extensive knowledge and experience about the environment in question.

To achieve this goal that must be looked upon as a long-term activity, a continuous undertaking aimed at building and sustaining a security-positive environment has to be emphasized.
All work concludes that the human side of enterprise – people is important. It is crucial to the effectiveness and success of an Information security policy that the security policy reflects the culture of the organisation. This ensures that the policy is seen as the organisation's own and goes a long way in the users' committing and adhering to it.

Findings from Chapter 2.4
Finding 2-12. Even common sense security measures reduce productivity
Finding 2-13. The level of defence is a risk probability decided by the management
Finding 2-14. Human error rather than flawed technology is cause of the security breaches
Finding 2-15. Address human side of the enterprise
Finding 2-16. Focus culture aspects of the organization
Finding 2-17. The "real" threats are often from within
Finding 2-18. Awareness is important
Finding 2-19. Security is a learned behaviour
Finding 2-20. It is essential to pose extensive knowledge and experience about the environment

2.5 What is an effective security policy

In our work, we have to establish a foundation for what we mean with the definition "effective" when we speak about a security policy. In addition, this question is experienced vague in nature due to the lack of papers found on what an effective security policy is proposed to be.

Analysis show that the degree to which users conforms to security mechanisms depends on their perception of security levels, information sensitivity and compatibility with work practices.

> "Security mechanisms incompatible with these perceptions may be circumvented by users and thereby undermine system security overall. It is therefore of great interest to identify the adequacy of in-place security policies, controls, and procedures and find out in to what extent a policy is effective in regulating the practices described." [Adams & et.al 1997] *p.1*

From literature survey, we found these statements about "effect" related to security policy:

> "However what is an effective information security policy? In the Oxford Dictionary of Current English, effectiveness is defined as "producing the desired results". In business terms, managerial success is measured against effectiveness, i.e. to achieve the organization's business objectives. Again, effectiveness is expressed in terms of achieving a certain result. Applying these definitions to an information security policy would thus mean that an effective information security policy assists in achieving the information security objectives of the organization". [Höne, Eloff 1/2002] *p.2*

From the literature survey, we look at Rosemary Sumajit [Sumajit 2002] *p.9* who argues that in order to make security successes within an organization, tools are needed that have nothing to do with technology at all:

- Executive-level backing
- Cooperation and input of everyone in the organization
- Organizational-wide discussions and training

These statements is necessarily not the complete answer in strive to find the key factors in making information security policies effective.

(ny) No matter how, the challenge the corporate management approach is to gain a fundamental apprehension of the security policy vision and mission in which they can enter a situation of handling the security objectives in an controlled and effective way.

In the document “How to write an Information Security Policy” Department of Trade and Industry, UK [DTI 2003] *p.8* the paper states in the Summary:

- Writing a policy is easy. Implementation can be more difficult.

2.5.1 Effectiveness

In report “A Systemic-Holistic Approach to Academic Programmes in IT Security” [Yngström 1996] L. Yngström discuss efficiency for Infosec systems in a certain environment. The definitions of efficiency and effectiveness used in the report is interesting. Yngströms refers to among others a definition from [Drucker 1973] *p.45*. “Definition of Efficiency is concerned with doing things right. Effectiveness is doing the right things.”

In the report [Yngström 1996] *p.65*, Yngström concludes:

> “Although there might be different ideas about which actual goal to control towards in a specific situation, there is some sort of consensus that there are choices to be done in some sort of order; firstly to choose to do the right things – then to do each one of them in the right way; thus to start with effectiveness followed by efficiency.”

Related to our work with Security policies it can be asserted:

- Speaking about making a security policy effective we are talking about starting to do the right things.

But knowing what the right things are seems to be the ultimate key question, which most likely is not possible to answere in its completeness. Anyhow awareness of the fact that the security objectives specified in the security policy is vital for the effectiveness due to the security work, and hence corporate results is important to keep in mind.

In finding out what makes a security policy effective and what to include in the definition of effectiveness, we have to reflect our statements again:

- Corporate strategy is about reaching a goal with least difficulty and in least time. Security is responsible for that the goal is met without disruption or harm and without fear of disturbance or injury.

To accomplish these factors a thorough understanding of the corporate issues has to be well known. Working with information security involves the whole spectre of human and technological disciplines at all levels within the organization. Writing an information security policy due to effectiveness requires skill and knowledge about the organization objectives and its particular strengths and weaknesses.

However, it is rarely found that we are handling just one goal or objective - in such, highly relevant due to our work with security policies. The security policy handles several objectives continuously and their prioritizing is most likely frequently changed pursuing the corporate objectives.

In terms of effectiveness, we are facing a situation whether to focus on distinct and short time goals, or to emphasize on more long-term objectives more related to the definitions “manage” and “mature” or maybe both.

It is easy to measure effect related to one distinct objective. However to ensure that the appropriate and correct long term objectives are defined and met is a more complex challenge.

In speaking about long term effectiveness related to security policies we are required to ensure a robustness lasting for weeks, months, years coming in the scope that:

- “the corporate objectives are met without disruption or harm and without fear of disturbance or injury”.

In this light, definition of measuring effectiveness must ascend from a somewhat specific situation to a functional level. We are talking about measuring effect in a system that:

- embraces a number of functions,
- operates in a dynamic environment,
- faces unpredictable threats.

Among others, W.G. Bennis [Bennis 1962] *p.7* presents the ideas about long term effectiveness to be defined by the organizations capability to manage problems, adapt to changes, maintain its activity and mature. This in relation to the more traditional ways by measuring effect related to static goals and results, even though useful information at appropriate levels.

As an alternative to measure results and satisfaction at a given point, Bennis introduces the more general definition “health”.

1. Adaptility to changes reflects the capability to solve problems, react flexible due to environmental changes.
2. A feeling of identity, which reflects the organizational knowledge of the objectives and principles in question.
3. Capacity to verify the realities due to environments characteristics and particular skills.
4. Integration which is a basis for the other three and maintains that the organizations different environment don’t (work against)counteract each other.

The right ting (effectiveness) is not to hardcopy another corporate security policy, but reflecting the organizational needs seriously, evaluating what can be done in the aim of achieving:

- Adaptability to changes,
- Feeling of identity,
- Capability to verify the realities,
- Inside integration

2.5.2 Efficiency

As stated above "efficiency" is concerned with "doing things right" which leads towards organizational environment and human beings.

Starting with doing the right things, a glance to the organizational theory most likely should be a good idea. The book "Organisasjons-psykologi" [Schein 1983] *p.21* defines one of the characteristics behind the definition of society:

> "Mutual help trough coordinated activities"

If coordination of activities shall gain any effect, it has to be defined some goals or results to accomplish, and that it does exist a fair possibility to reach these goals or results. Another important idea behind the principle of organization is therefore the idea about reaching specified mutual results through coordinated activities

> An organization is a systematic coordination of people's activities to obtain a mutual clearly defined objective, through dispersion of work and functions, through a hierarchy of authority and responsibility [Schein 1983] *p.25*[8].

It may be asserted that writing a security policy, which is effective:

- Is about focusing on the right things (objectives) and specify the objectives in a way that can be accomplished, and that it does exist a fair possibility to reach these goals or results in an efficient way.

If a person, a group or e.g. a corporation - aims toward a distinct goal, it is a possibility to measure the progress related to that specific goal and hence obtain a picture of the efficiency.

Effectiveness is measuring/monitoring a level made up of a number of goals or objectives, in which each of them has to be efficient

In security work, it seems appropriate to keep in mind the difference between effectiveness and efficiency due to the task responsibility within the organization. Effectiveness points at the management in "starting to do the right things". Efficiency is an organizational objective related to the objectives specified to be accomplished. - "mutual help trough coordinated activities"

[8] All statements from the book is translated from Norwegian by author of this paper

2.5.3 Structure and levels supports effectiveness and efficiency

Literature point of the importance that all organizational activities involved is coherent and structured in a way that supports structure of the organization hierarchy and the business and security objectives. It is important to be aware of these principles due to implementation of security policies in general. Policies may range from high-level i.e. abstract non-technical policies to low-level policies, depending on how the desired behaviour of the managed resources is specified.

René Wies in the paper "Using a Classification of Management Policies for Policy Specification and Policy transformation" maintain that to be able to guarantee that all policies are applied to their target (provided they are not in conflict with each other), it is essential to structure these policies. Thus, a policy hierarchy is a way of splitting the vast number of policies into smaller groups of different levels of abstraction, which can be further processed in distinct steps and transformed into applicable low-level policies.[Wies 1995] *p.6-7*

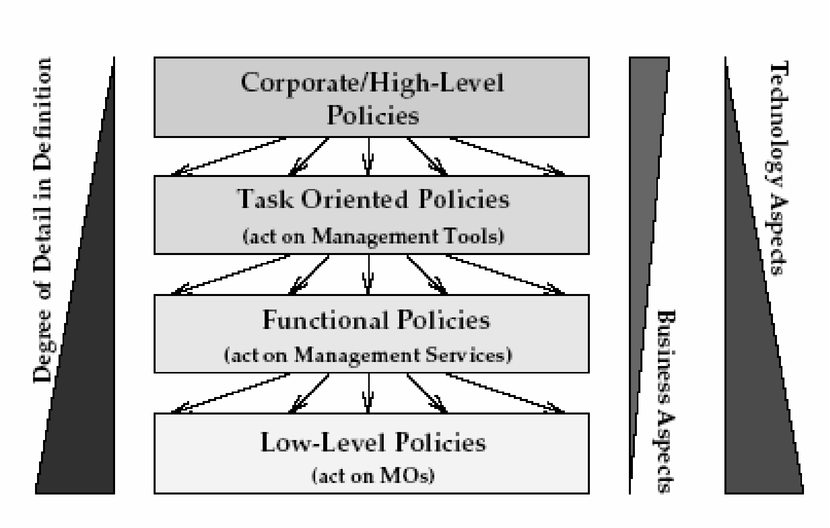

Degree of Detail in Definition
Corporate/High-Level Policies
Task Oriented Policies
(act on Management Tools)
Functional Policies
(act on Management Services)
Low-Level Policies
(act on MOs)
Business Aspects
Technology Aspects

Figure 2-2. The policy hierarchy

Thus, a policy hierarchy defines the levels within the management environment at which policies are applied. As the Figure illustrates, the policy hierarchy distinguishes between corporate policies, task oriented policies, functional policies and low-level policies.

Corporate policies or high-level policies are directly derived from corporate goals and thus embody aspects of strategic business management rather than aspects of technology-oriented management. To allow their application within the management environment, they have to be refined to one of the three policy types as shown in Figure 2-2. [Wies 1995] *p.6*

Such a structure assists the findings related to effectiveness and efficiency in the way that the high-level policy focus on the security objectives (doing the right things) and that the lower level policies focus on efficiency (doing things right).

Other examples of policy hierarchies can also be found. The Critical Infrastructure Assurance Office (CIAO) [CIAO 2000] in a report goes on to identify three types of policies based on NIST standard 800-14, distinguished by Program policy, System-Specific policy and Issue-specific policy.

2.5.4 Anchoring the policy

From organizational theory comprehensive research related to structure, processes and culture are important knowledge in the aim to accomplish effective information management systems. An organizational structure can be defined as the sum of ways in which tasks are defined into separate activities and coordinated in the aim to obtain a result. A control chain that transforms the strategy into the actual organizational levels as shown in the simplified figure obtains this.

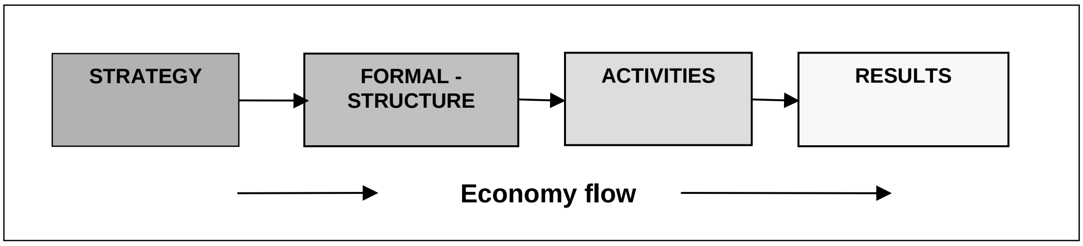


Figure 2-3. Control chain from strategy to results

In this chain, the formal structure will be an important factor in the aim to transform the strategy into the organization levels. Weakness in translation process may lead to shortcoming in the aim to achieve the desired results specified. From an architects point of view the formal structure is an essential question about analyzing, systemising and assigning tasks in a way that ensure the long term strategy. [Fivelsdal, Bakka 1998] *p.50*

The “formal structure” transforms the corporate strategy defined into objectives **(why necessary)** described in the high-level policy. Using the described policy hierarchy each objective can be further detailed into principles **(what needs to be done)** to allow a stepwise refinement of the policy.

The lower the level of abstraction, the more precise and detailed will the definition become, i.e. the granularity of the criteria increases leading to **(how to do it)**.

This is illustrated with help from a figure showing the strategy, organization and architechture hierarchy illustrated in the book “Håndbok i datasikkerhet”. [Daler, Gulbrandsen, Høie, Melgård, Sjølstad 2002] *p. 223.*

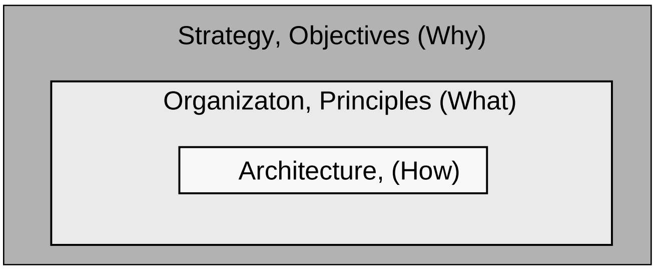


Figure 2-4. Formal structure, which transform the strategy into organization levels

The high-level policy is important in the light of its duty to define objectives and tie objectives and principles together, and orchestra all activity hence to information security in the organization. However the way an organization is structured varies of course related to the activity and size of the corporation and must be taken into consideration.

For example, a high-level policy calling for a weekly backup of all the company's data may be refined to specify the backup media for different workstation cluster and identify the system administrators that are responsible for operating stackers or changing tapes. [Wies 1995]

2.5.5 How to know that SP ensures effectiveness and efficiency

The requirement to measure IT security performance is driven by regulatory, financial, and organizational reasons. A number of existing laws, rules, and regulations cite IT performance measurement in general and IT security performance measurement in particular, as a requirement.

The area of measuring security has been a crucial topic for long time and use of security metrics has gained serious interest the past years. The concept or discussion point related to measuring security is: What are we trying to achieve? Voices in the workshop conducted by NIST June 2000 [Nielsen 2000] indicated that we need something simple and effective that "tells the story".

NIST, Special Publication SP800-55, Security Metrics Guide for Information Technology Systems, July 2003 [NIST 800-55] provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate non-productive controls.

In paper using security metrics to assess risk management capabilities [C.Kormos & et.al 1999], Kormos argues that measuring security effectiveness is a challenging enterprise. Metrics cannot be used productively without understanding the relative importance of system security for the organization's mission. The selected metrics should be relevant to the organization's business areas. The paper discusses the challenge in measuring the short and long time objectives approaching it from two different perspectives.

It is therefore of great interest to identify the adequacy of in-place policies, procedures and security controls and find out in to what extent a police is effective in regulating the practices described.

Findings from Chapter 2.5
Finding 2-21. User's perception of security- levels, sensitivity and work practices is important
Finding 2-22. Cooperation and input of everyone in the organization is important
Finding 2-23. Organizational-wide discussions and training is important
Finding 2-24. An effective security policy starts with doing the right things
Finding 2-25. Understand the organization objectives, strengths and weaknesses.
Finding 2-26. Measure static goals "economical results"
Finding 2-27. Measure Level of robustness "health"
Finding 2-28. Define "to the point" goals that can be accomplished
Finding 2-29. Ensure that it exist a fair possibility to reach goals and results
Finding 2-30 Structure and levels supports effectiveness and efficiency
Finding 2-31. To determine effectiveness and efficiency something has to be measured

2.6 Less research on the subject

In the search for documentation about security policies, a well of information is accessible. However, most of the documentation found is about design and development of different lower level policies mostly seen from a theoretical and technical view.

The paper "A simple classification model for research in information security"[Yngstöm, Björck 2000] supports this experience were 125 papers published on the proceedings of the IFIP World Computer Congress/SEC 2000 were examined. The result of the analysis showed inconsistency between the current problems regarding information security in organisations today and the focus of the 125 presented papers. The outcome suggests that more emphasis should be placed on research on issues on 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.

The Paper "A Framework for Information Security Culture" [Kufås 2002] *p.1* is focusing on experiences from the Norwegian offshore industry and the work within the context of "safety" and that much focus has been on safety culture and other organizational factors. The report maintains that according to the insider problem of information security, there is a need for research on cultural aspects and their contribution to human behaviour.

In an article "Why there aren't more information security research studies" [Kotulic and Clark 2003] describes an attempt to conduct an experiment in the area of security risk management (SRM) with purpose to create and test a conceptual model of SRM program at the firm level.

The research study was not able to collect enough data for statistical significance. Their conclusion was that the organizational information security domain is relatively new and under researched. In spite of this, it may prove to be one of the most critical areas of research necessary for supporting the viability of the firm.

2.7 List of Findings

2.8 Summary State of the art

The Information security policy is a document with the purpose of providing management support and direction for information security.

- Corporate strategy is about reaching a goal with least difficulty and in least time. Security is responsible for that the goal is met without disruption or harm and without fear of disturbance or injury.

It is not easy from examination of the professional's documentation and literature to understand what a security policy is really about. The documentations are also emphasizing different aspects, and the message communicated apprehends occasionally vague and not consistent.

It is noticed that the international security standards is not necessarily entire in the guidance of how to write and implement a security policy.

Disruption, harm, and disturbance represent a threat to the organization and their systems. Security is about protecting values from threats, which is likely to:

- Emerge from both outside and inside the enterprise.

Security shall ensure protection of corporate objectives in motion, which implies that:

- Securing assets is a continuous 24 hour process which is never finished

Economy is stated to be a decisive factor and that security in most cases is a risk-based activity.

Writing an effective Information security policy requires knowledge and experience in having full understanding of the organizational objectives and its particular strengths and weaknesses.

All work concludes that the human side of enterprise – people is important. It is crucial to the effectiveness and success of an Information security policy that the security policy reflects the culture of the organisation.

It may be asserted that writing a security policy, which is effective is about:

- focusing on the right things (objectives) and specify the objectives in a way that can be accomplished, and that it does exist a fair possibility to reach these goals or results.

An accepted management principle is that an activity cannot be managed if it cannot be measured. Security falls under this headline. Because IT governance is about alignment with business objectives, metrics should be developed and reported within a business context.

The performance of IT security must be measured over the long haul, and metrics that are business-relevant should be captured.

From the list of Findings revealed from this chapter, a selection of factors assessed as essential is listed. These factors in addition with the finding found from the questionnaire forms a basis for further analyses.

3 THE SURVEY

The grand aim of all science is to cover the greatest number of empirical facts by logical deduction from the smallest number of hypotheses or axioms.

-Albert Einstein

3.1 Questions of interest

A majority of all findings from the literature survey points in the same direction. Making a security policy effective is an embracing and challenging task. Papers discussing the issue emphasize the importantance of the human factor and argues that in order to make security successes within an organization, tools are needed that have nothing to do with technology at all. The papers found indicate that the human side should be focused.

Factors that repeatedly mentioned points at:

- Corporate goals and objectives
- Assets and threats
- Balancing security issues and interests
- Economy, financial loss, fraud, unauthorized use
- Vulnerability, resistant to threats, quality
- Human factor, Insiders,
- Executive-level backing
- Cooperation and input of everyone in the organization
- Organizational-wide discussions and training
- Motivation and awareness
- Levels, structure and processes *(ny)*
- Monitoring ,measuring, reporting, following up
- Need of extensive knowledge and experience about the environment
- Users often lack knowledge of the Policy's existence

Numerous surveys[9] are carried out to disclose financial losses, threats, security breaches, and criminal activity. However, no papers are found describing practical research on what effect embraces and what factors influencing it.

What is of primary interest for us is to gain knowledge of the definition "effective". What is effectiveness in a security context? What factors of importance influence it?

The aim is to get a picture of key factors that makes the security policy being an effective course of action in pursuing and support of the corporate objectives.

[9] Department of Trade and Industry (DTI), Pricewaterhouse Coopers (PWC), Information security breaches (2004), CSI/FBI Computer crime and Security survey (2003), Symantec, Symantec Internet Security Threat report (2003). Næringslivets sikkerhetsorganisasjon (NSO), Mørketalls undersøkelsen (2003).

3.2 Practical accomplishment of the survey

> "There is no "golden formula" which, if slavishly adhered to, will ensure success and fend off all potential criticisms. Almost inevitably, the researcher will need to apply discretion, make trade-offs and exercise judgement when producing and implementing a questionnaire." [Denscombe 2003] *p.144*

3.2.1 Approach

The purpose is that the survey should be good enough to:

- *develop relevant true statements, ones that can serve to explain the situation of concern or that describes the casual relationships of interest.*

If the problem is identifying factors that influence an outcome, the utility of an intervention, or understanding the best predictors of outcomes, then a quantitative approach is best. It is also the best approach to use to test a theory or explanation. On the other hand, if a concept or phenomenon needs to be understood because little research has been done on it, then it merits a qualitative approach.

In the nature of the fact that the courses of action in compiling a security policy will depend on many factors and in a great extent will vary from organization to organization the method chosen must be able to reveal (fundamental) general problems (facts). Work in the project plan revealed that a lot of theory about the subject was available, but reports describing practical work or results were rarely seen.

It is well known that many organizations are restrained in answering questionnaires about security related issues. The State of the art also supports this (ref. Chapter 2.6). To achieve information appropriate for our use it seems recommended to conduct the survey in a way that offers full anonymity.

In an initial phase, a quantitative method, which surveys a number of organizations for information, seems to be the best entrance in solving the question.

It was emphasized to reach big organizations with the assumption being in a position that it is important that the corporate objectives can be met without disruption or harm and without fear of disturbance or injury. Focusing this type of organizations was considered to be of interest in the light of reaching organizations with experience and a certain level of maturation due to work with security.
The questionnaire should provide a basis to conduct an appraisal of an organization's information security status and factors influencing it. To achieve this and in to an extent possible, phrase the questions in a way that makes it possible to hold different parameters researched up against each other.

The surveys mentioned focuses on the financial loss from unauthorized activity that of course is of interest.

However, it should not be forgotten that the content of definition “Loss” embraces more than only financial values.

As discussed the aim with security work is that the corporate objectives can be met without disruption or harm and without fear of disturbance or injury. This statement includes in addition to loss of money also loss of values related to corporate sensitive information, privacy issues and e.g. being a remedy for criminal acts or relaying malicious code.

The ability to process the daily work without disruption and harm is outmost important in the light of reaching contracted agreements with other partners settled e.g. in Service Level Agreements (SLA’s). Lack of performance most often release requirements for considerable compensations gaining direct influence at the bottom line. Assessing loss due to some of the factors mentioned may be difficult.

3.3 How the survey was conducted

The survey is based on questionnaire sent to the Security Officer (SO) in forty-one “large” organizations. The definition of a “large” organization varies depending on geographical location; however, in Norway a “large” organization is defined to employ more than 100 persons. In Europe (EU countries) or in US the level on what considered being a “large” organization may vary between 200 and 250 employees.

As mentioned, it is well known that many organizations are restrained in answering questionnaires about security related issues. The survey therefore was conducted in a way that offered full anonymity. This was done by use of a postal questionnaire were it was focused on formulating the questions in a way that should be impossible to track the respondent. The respondent received together with the questionnaire an envelope ready named and stamped by a postal franker which also gained anonymity due to geographical location envelope sent from.

To avoid questionnaire-received cold, every SO was phoned before, or very near to receiving of the questionnaire to inform about the purpose. However two SO’s were not reached. The questionnaire was sent enclosed with a cover letter, which informed about the purpose of the survey.

3.3.1 Pilot

From start, the project plan included an arrangement in approaching the security officer (SO) and a number of employees in each organization. The intention was to evaluate management statements against viewpoints from ICT professionals and users. Questionnaire was formed and piloted in one company. The result was however not very edifying with an employee response rate on 33%. The plan was to send questionnaire to twenty organizations reaching the SO and fifteen employees in each of those organizations.

This plan was terminated due to the low response rate and uncertainty in getting adequate material for examination.

It was then decided to reformulate some of the questions in the SO's questionnaire and focus on SO only. The population was increased to forty-one organizations. This questionnaire was piloted in two organizations within ErgoGroup gaining comments of great value.

3.3.2 The population

The definition of a security policy contains a variety of meanings. The thesis concentrates on security policies for organizations where Information and Communication Technology (ICT) is of high importance for the daily operation.

The questionnaires was sent to a broad sphere of organizations within official government, health sector, competitive IT related companies within different segments, big counties, official directorates, PTT companies, power suppliers, bank and financial organisations, insurance companies, educational organisations, and some companies within special trades.

Most of the directed organizations is assessed being in a situation requiring adequate need of security in the aim that corporate objectives can be met without disruption or harm and without fear of disturbance or injury. One question reflected to what extent the organisation was subject to official legislations or directions.

Regulations and directives:		63 %	21 %	13 %	4 %	0 %
Regulations and directives:		Very high	High	Less	Very low	Can't answ.
		15	**5**	**3**	**1**	**0**
Does the organization work with information regulated by official law (directives) that influence design and operation of the ICT systems: Personal data act 2000, "Kredittilsynets IKT forskrift", "Forvaltningsloven" etc.	24	15	5	3	1	0

Table 3-1. Question and number of answers due to subject legislation and directives

Of total twenty-four respondents, twenty of them (83%) answered "Very high" or "High" on this question. Four respondents answered "Less" or "Very low" (19%) of the total population.

All the organizations are rated as "large" hence to Norwegian scale for sizing organizations. Most of the organizations are rated "large" also compared with European or US measures. All organizations reported having security policy in place.

It's an overweight of respondents focusing on economical results. Sixteen compared to eight which represents a selection of respondents covering different objectives and cultures.

Focused on economic results:		33 %	27 %	21 %	19 %	
Focused on economic results:		Very high	High	Less	Very low	Can't answ.
		16	**13**	**10**	**9**	**0**
Is the organization that you are working in focused on economical objectives and results?	24	9	7	6	2	0
In our organization many of the employees are evalutated against economical results.	24	7	6	4	7	0

Table 3-2. Results "Focused on economical results" (all respondents)

3.3.3 The questionnaire

The questions in the questionnaire were mainly based on the work from state of the art. In addition advisory from SO's within the Ergo concern was taken into consideration.

In the preliminary phase of the work, factors reflecting the outline of the policy were emphasised.

- Will the questions cover the full range of issues?
- Are we measuring what we think we are measuring
- Are we measuring what we intend to measure
- Will the research produce true and honest findings?
- Will the data be precise and detailed?
- Are respondents likely to give full and honest answers?
- Will the investigation manage to focus on the most vital issues?
- Will an adequate number and suitable diversity of people, events etc. be included?
- Will it be reasonable to generalize based on the data collected?
- Is it likely that there will be an adequate response rate?
- Short and precise questions as possible

The questionnaire was designed with use of interval scale- ordinal with distinct intervals. The questionnaire is designed in the aim that the measurements give a "fair" picture of the variable being measured.

3.3.4 Questions reflecting "effect"

As found in the literature study, the security policy is one of the most important controls in management of security. The first step of interest to investigate is to find out what "effect" the security policy produce within the environment questioned.

If differences reveal within the population we will look for parameters that most likely influence the produced "effect". The first question related to effect and security policy is:

SP performs weaker effect than expected:
Has the security policy weaker effect than expected in your organization?

Figure 3-1. Questions asked regarding effect of the security policy

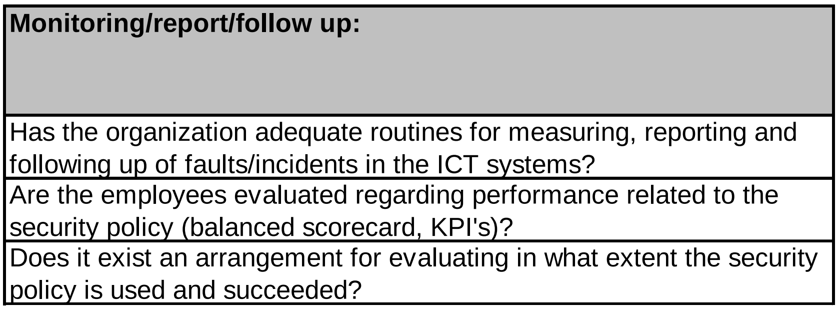
This question is also followed up with a control question:

Do you experience conformity between what is written in the security policy and practical experience in your organization

Figure 3-2. Control question to Figure 3-1

The reliability and validity of reported results regarding this question can be questioned from the point of view that it is a subjective comprehension, not based on a common platform of measurements. To reduce this uncertainty we questioned whom of the respondents that possess arrangement for evaluating in what extent the “Security policy is used and succeeded”.

This question is one out of the three questions in parameter “Monitoring/report/follow up”.



Monitoring/report/follow up:
Has the organization adequate routines for measuring, reporting and following up of faults/incidents in the ICT systems?
Are the employees evaluated regarding performance related to the security policy (balanced scorecard, KPI's)?
Does it exist an arrangement for evaluating in what extent the security policy is used and succeeded?

Figure 3-3. Questions asked regarding “Monitoring/report/follow up”

The purpose with a security policy is to specify the security objectives in such way that the enterprise goals are met without disruption or harm and without fear of disturbance or injury.

As mentioned, it may be asserted that writing a security policy, which is effective, is about:

- Focusing on the right things (objectives) and specify the objectives in a way that can be accomplished, and that it does exist a fair possibility to reach these goals or results.

After all, the intention with the security policy is to establish an environment, which is resistant to present and potential threats.

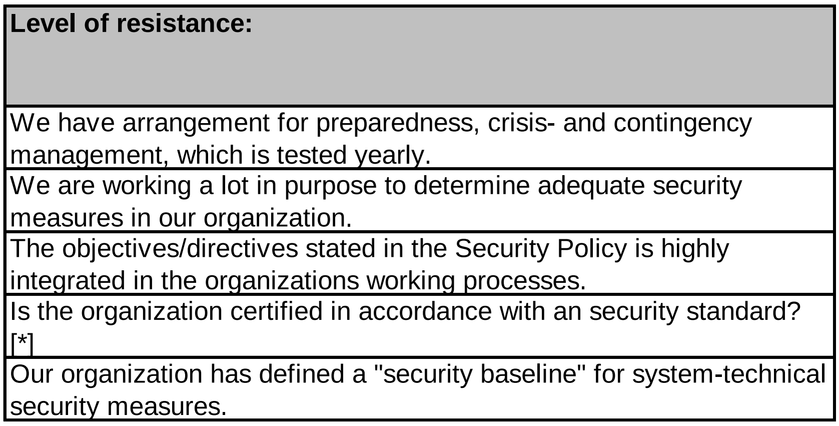
The definition of security policy implicit entails that the main task is to produce a “Level of resistance” appropriate in the aim of avoiding fear, disturbance or injury in the daily work

It is assessed interesting to look for characteristics related to the “Level of resistance” factor and the questions phrased is one point of view of what “Level of resistance” could be.

Based upon the findings about focusing on the right things (objectives) and specify the objectives in a way that can be accomplished, the factor “Level of resistance” is composed of a set of questions reflecting effectiveness[10]. Each of these questions related to effectiveness is considered important in avoiding impact from threats reflecting professionalism and engagement in security work.

A good score should entail robustness and fit for fight in avoiding threats in both a short and long time horizon.

[10] Doing the right things



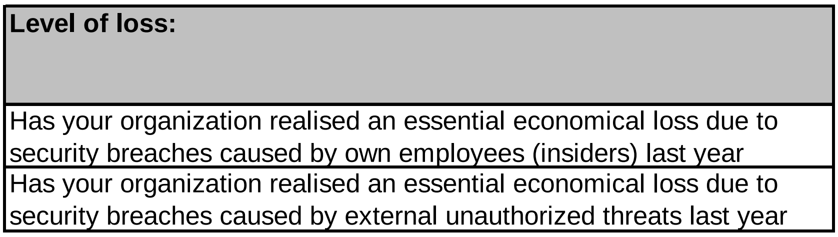
Level of resistance:
We have arrangement for preparedness, crisis- and contingency management, which is tested yearly.
We are working a lot in purpose to determine adequate security measures in our organization.
The objectives/directives stated in the Security Policy is highly integrated in the organizations working processes.
Is the organization certified in accordance with an security standard? [*]
Our organization has defined a "security baseline" for system-technical security measures.

Figure 3-4. Questions asked regarding “Level of resistance”

The scope of “effect” is as mentioned in chapter 2.5 embracing, and it was decided to phrase a question to disclose to what extent the respondent has experienced economical loss in a short time horizon.

It is also natural to expect that the value of economical loss related to security breaches should be reflected due to the value of “Level of resistance”.

Economical loss due to security breaches is at “the end” the parameter that governs the security effort. Serious incidents will most likely affect the enterprise economy indicating to what extent a security policy is effective.



Level of loss:
Has your organization realised an essential economical loss due to security breaches caused by own employees (insiders) last year
Has your organization realised an essential economical loss due to security breaches caused by external unauthorized threats last year

Figure 3-5. Questions asked regarding “Level of loss”

The questions regarding “effect” mentioned in figure 3-1 to 3-5 are grouped in following segments shown in table 3-3.

Questions related to effect of the security policy	**1 question**
SP performs weaker effect than expected	1 question
Questions related to organizational effectiveness	**7 questions**
Level of resistance/robustness	5 questions
Level of loss	2 questions

Table 3-3. Questions related to effect

3.3.5 Parameters anticipated to influence "effect"

The parameters decided to examine is primarily human related due to findings from our literature study. As argued in the paper [Sumajit 2002] *p.9* to make security successes within an organization, tools are needed that have nothing to do with technology at all:

- Executive-level backing
- Cooperation and input of everyone in the organization
- Organizational-wide discussions and training

Factors which preliminary seemed to be of interest are conditions related to outline and communicating the policy. However, the literature study points at the importance of human related issues. Factors of importance mentioned are "engagement from the management", "learning/awareness problems", "monitoring", "cultural aspects" related to behaviour and attitude, and "focus on economical results".

The intention is to make a "framework" embracing parameters supposed to influence the "effect" of the security policy and organizational robustness.

The "parameter framework" (see table 3-4) as examined in "chapter 4 Findings" contains factors which, most likely influence "effect" on the security policy and organizational robustness ("Level of resistance").

Parameters supposed to influence "effect"	**19 questions**
Personal bonding/networking	1 question
SP based on common standards/"best practices"	1 question
Learning (awareness)	3 questions
Focus on economical results	2 questions
Monitoring (measuring/reporting/follow up)	3 questions
Focus on behavior and attitude (cultural aspects)	4 questions
Engagement from management	5 questions

Table 3-4. Parameters supposed to influence effect

3.3.6 Causes to security breaches

To limit the extent of the work it was considered necessary to limit the examination area. This was done by researching causes that most likely leads to security breaches due to the security policy (see table 3-5).

What causes security breaches related to the SP	**3 questions**
Lack of respect related to security policy	1 question
Lack of knowledge related to security policy	1 question
Poor design of security policy	1 question

Table 3-5. Questions reflecting causes to security breaches

The postal questionnaire was for this reason made with some entropy hence to number of questions. Dependent on the reported answers, the most pronounced causes to security breaches related to the security policy was examined. Hence, relevant questions and their answers are drawn upon. E.g., the respondents have reported that "outline of the security policy" seems to be the least important factor due to security breaches. The seven questions in the postal questionnaire affecting this area are of this reason not further examined, and left behind.

The postal questionnaire contains forty-three questions. At the end, the basis for examination shown in the tables at most involves thirty of the questions with belonging answers.

Some questions asked are of informational and supportive character. [11]

Informative questions	**4 questions**
Number of employees in organization	1 question
Embraced by official legislations	1 question
Dependency of key personal	1 question
External sources for knowledge of threats	1 question

Table 3-6. Informative questions

3.3.7 Ethics

The ethical question has to be taken into consideration. Surveys that affect security issues may reveal information that can make the involved organizations vulnerable. The identities and the interests of those involved shall be protected. Findings that could compromise one or more companies should not be disclosed.

It is a question of integrity and confidence to guarantee the confidentiality of the information given the research.

3.3.8 Realibility and validity

The selection was done among Norwegian companies with more than 100 employees ("large" organizations) where ICT is considered to be of vital importance for the daily operation.

The survey is primarily directed at companies assessed to gain interest in adequate security and selected pseudorandom. Most of the selected organizations operate within fields that must be considered to be of vital interest of the community. The selection of respondents is to a certain extent selected on personal knowledge and judgement and suggestions from relevant advisors in which companies could be of interest.

There are of course more companies to address within the scope of this assessment. However, time and resources in the scope of keeping the project plan and optimism in approaching thirty respondents stopped dispatching questionnaires at a number of forty-one. The business sphere taken into consideration an approached response rate on 59% is considered fair.

[11] The framework showing parameters and their related questions is enclosed in Appendices.

Literature concludes that samples should not involve fewer than thirty people or events. Certainly, it is a mistake to use statistical analyses on samples of fewer than thirty without exceptional care about the procedures involved. Further, it is not acceptable to present the findings of small surveys as percentages without specifying the actual numbers involved. [Denscombe 2003] *p.24*

The answers are at most presented shared according to percentage and the actual number involved.[12] The received material is considered to sparse too be of interest for extensive statistical analysis.

The validity of the survey is however considered being good. The questions are closed and the respondents represented by security officers are characterized by their skill and accurate knowledge of the security sphere. Anonymity increases the possibility for reliable answers.

The measurements are considered reproducible. The answers are real and reflect the situation of the organizations in question.

The received material contains nevertheless information of interest. The findings are presented in column diagrams. Conclusions are drawn from expressive variances seen.

[12] In cases figures are not shown these are documented in the appurtenant Appendices

4 FINDINGS

The proper study for mankind is man

- Alexander Pope

4.1 Accumulated results all respondents

Table 4-1 shows answers shared according to percentage covering all organizations, totally twenty-four respondents.[13]

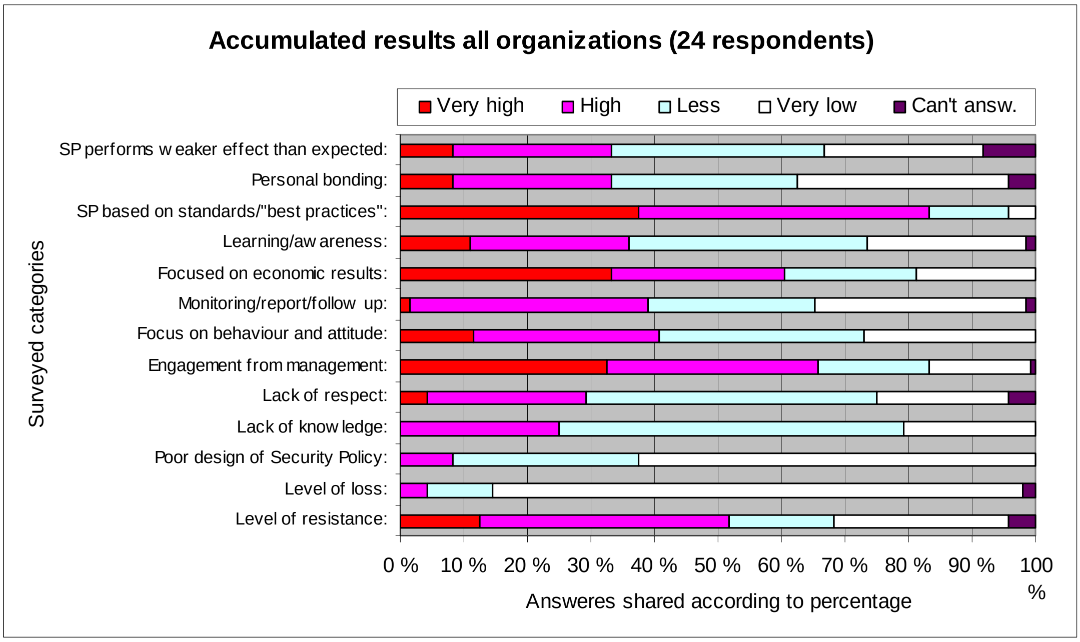


Table 4-1. Diagram "Accumulated results all respondents"

Table 4-1 illustrates the "total framework" containing thirty questions grouped as shown in tables 3-3 to 3-5. "Effect" from security policy is located at top of the diagram. Questions related to "Level of loss" and "Level of resistance" at the bottom.

The "can't" answer alternative is considered important as a reflection due to which of the factors that was problematic to answer. The questions related to "Effect", "Lack of respect" and "Personal bonding" gains the highest scores and may serve as indicators to what could be the challenges.

The answers reports that all organizations have security policy in place. Twenty of the respondents use standards or "best practices" in preparation of the policies.

[13] Results from the arrangements is enclosed in the appurtenant appendices

4.1.1 “Effect” of the security policy and “Level of resistance”

About “effect” from the security policy, eight respondents report that the policy shows “weaker effect than expected”, while fourteen respondents report that the policy is “not weaker than expected”, (two respondents cannot answer).

SP performs weaker effect than expected:	8 %	25 %	33 %	25 %	8 %

SP performs weaker effect than expected:		Very high	High	Less	Very low	Can't answ.
		2	**6**	**8**	**6**	**2**
Has the security policy weaker effect than expected in your organization?	24	2	6	8	6	2

Table 4-2. Results “Security policy performs weaker effect than expected” (all respondents)

The graph “Level of resistance” gains a good score. These “effectiveness” questions represent security work that requires high involvement and endurance over time.[14] Looking at the graph the overall conclusion must be that robustness (“Level of resistance”) for the organizations as an average must be considered as good.

Level of resistance:	13 %	39 %	17 %	28 %	4 %

Level of resistance:		Very high	High	Less	Very low	Can't answ.
		15	**47**	**20**	**33**	**5**
We have arrangement for preparedness, crisis- and contingency management, which is tested yearly.	24	4	11	5	4	0
We are working a lot in purpose to determine adequate security measures in our organization.	24	4	13	3	4	0
The objectives/directives stated in the Security Policy is highly integrated in the organizations working processes.	24	2	14	5	3	0
Is the organization certified in accordance with an security standard? [*]	24	3	0	0	19	2
Our organization has defined a "security baseline" for system-technical security measures.	24	2	9	7	3	3

Table 4-3. Results “Level of resistance” (all respondents)

It is difficult to draw any conclusion out of these figures. However, an important condition for further work is the present differences within the population.

4.1.2 ”Level of loss”

The graph, “Level of loss” due to security breaches caused by internal employees or external unauthorized threats is not very significant. This finding harmonizes with findings done in other international surveys [ISBS 2004] *p.24* in which direct financial losses related to security breaches are reported “low”.

Level of loss:	0 %	4 %	10 %	83 %	2 %

Level of loss:		Very high	High	Less	Very low	Can't answ.
		0	**2**	**5**	**40**	**1**
Has your organization realised an essential economical loss due to security breaches caused by own employees (insiders) last year?	24	0	1	2	20	1
Has your organization realised an essential economical loss due to security breaches caused by external unauthorized threats last year?	24	0	1	3	20	0

Table 4-4. Results “Level of economical loss caused by insiders/outsiders” (all respondents)

[14] The table show answers shared according to percentage. The actual number is shown in table 4-4.

If we look at the figures and what is reported we find that losses reported “High” comes from two respondents and “Less” is reported from three respondents a total of five, which represents almost 20% of the group.

This figure is low compared to international and national surveys done. However, the low volume and selection of respondents taken into consideration may be an explanation.

It is reported two breaches causing economical loss rated “High”. One caused by an insider the other one an outsider. Economical loss rated “Less” is reported in five cases. Two breaches caused by insiders and three by outsiders. The rest of the respondent’s reports “Level of loss” to be “Very low”.

4.1.3 Causes to security breaches

The intention as mentioned in chapter 3.3.6 is to reveal which areas that is considered to be most vulnerable in the work with security policies. Three questions are asked in the aim to limit the search area.

What causes security breaches related to the SP	**3 questions**
Lack of respect related to security policy	1 question
Lack of knowledge related to security policy	1 question
Poor design of security policy	1 question

Table 4-5. Causes to security breaches related to the security policy

The result for all organizations (see table 4-1 and 4-6) indicates that the security officers do not experience that outline of the security policy is cause to security breaches to any extent.

Poor design of Security Policy:	0 %	8 %	29 %	63 %	0 %
Lack of knowledge:	0 %	25 %	54 %	21 %	0 %
Lack of respect:	4 %	25 %	46 %	21 %	4 %

Poor design of Security Policy:		Very high	High	Less	Very low	Can't answ.
		0	**2**	**7**	**15**	**0**
Have conditions due to poor design of the security policy been direct cause to security breaches during the last year?	24	0	2	7	15	0
Lack of knowledge:		Very high	High	Less	Very low	Can't answ.
		0	**6**	**13**	**5**	**0**
Have conditions due to lack of knowledge of the security policy been direct cause to security breaches during the last year?	24	0	6	13	5	0
Lack of respect:		Very high	High	Less	Very low	Can't answ.
		1	**6**	**11**	**5**	**1**
In what extent are security breaches traceable due to employees lack of respect for the security policy?	24	1	6	11	5	1

Table 4-6. Results “Causes to security breaches related to the security policy” (all respondents)

Two respondents reports “High” which represents 8% of the total.

It is of interest to observe that 83% of the respondents (20 out of 24) use standards or “best practices” in preparation of the policies.

SP based on standards/"best practices":	38 %	46 %	13 %	4 %	0 %

SP based on standards/"best practices":		Very high	High	Less	Very low	Can't answ.
		9	**11**	**3**	**1**	**0**
Is preparation of the security policy based on standards or "best practices" (e.g. ISF or equivalents)?	24	9	11	3	1	0

Table 4-7. Results “SP based on standards/”best practices””? (all respondents)

It is a considerable difference between the level reported related to “Poor design” of the security policy and the level reported for “Lack of knowledge” and “Lack of respect”.

“Lack of knowledge” is considerably higher, with six respondents reporting “High” and “Lack of respect” even higher with six respondents reporting “High” and two reporting “Very high”.

Whether these findings stand statistical analysis and is representative for a larger population is a question for further work. These findings are considered valid for the respondents in question.

It is of interest to notice the answer on one of the questions related to insider/outsider problems. Nineteen of the respondents agree that security breaches related to unintended incidents cause most of the security breaches.

		Very high	High	Less	Very low	Can't answ.
Can you agree on the assertion that most security breaches are caused by unmalicious incidents perceived as faults and accidents most likely caused by human errror	24	5	14	5	0	0

Table 4-8. Results “Security breaches are incidents caused by human error” (all respondents)

These findings support that the outline of the policy is the least significant cause, due to security breaches, which is incorporated in the present “parameter framework”.

4.2 Examining parameters related to "effect" of the SP

In the anticipation that the respondents emphasize "adequate security", we assumed an extent of heterogeneousity. The results received supports this assumption and the questionnaire revealed a considerable span in reported "effect" of the security policy and "Level of resistance" between the organizations asked.

The present span in "effect" of the security policy and "Level of resistance" offered the possibility to look at differences in the parameters under research.

4.2.1 Respondents reporting "Security policy weaker than expected"

"Effect" of the security policy is as mentioned rated to gain "weaker effect" than expected from 1/3 of the organizations.

Table 4-9 shows results related to the question "SP performs weaker effect than expected" which are answered with "Very high" and "High".

The response shows low rates on "Learning/awareness". This harmonizes with a "high" score on "Lack of knowledge", which is 50%.

The factor "Lack of respect" is present with 38%.

However, "Engagement from management" is good with almost 60% and "Level of resistance" is equal with the average for all respondents.

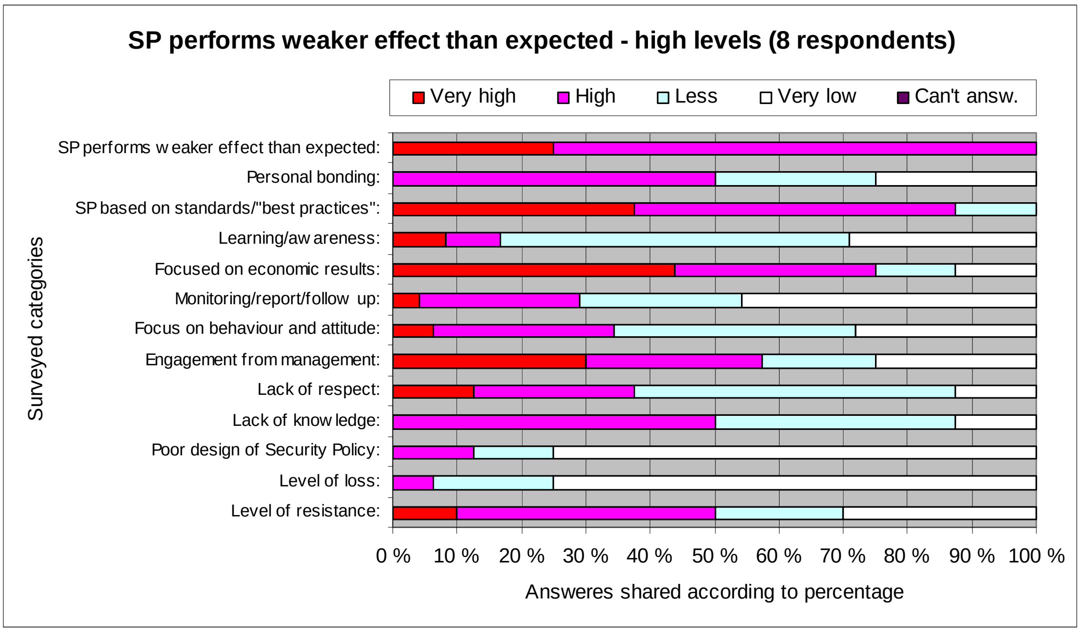


Table 4-9. Diagram "SP performs weaker effect than expected" (high levels)

4.2.2 Respondents reporting "Security policy not weaker than expected"

Examining the results from the group responding "security policy not weaker than expected" (respondents with "Less" and "Very low") show some interesting elements (see table 4-10).

The parameter "Learning/awareness" of the security policy increases. "Lack of knowledge" decreases and both parameters show a percentage difference with 30% and more.

It is also noticeable that "Engagement from management" is expressive higher. The parameter "Personal bonding" is lower in this group, but contains an element of "Very high" which is not present in the first group.

The "Level of loss" is reported low from both groups of respondents. The "Level of resistance" is reported slightly higher for the "SP not weaker group", and do not reflect any difference in robustness level.

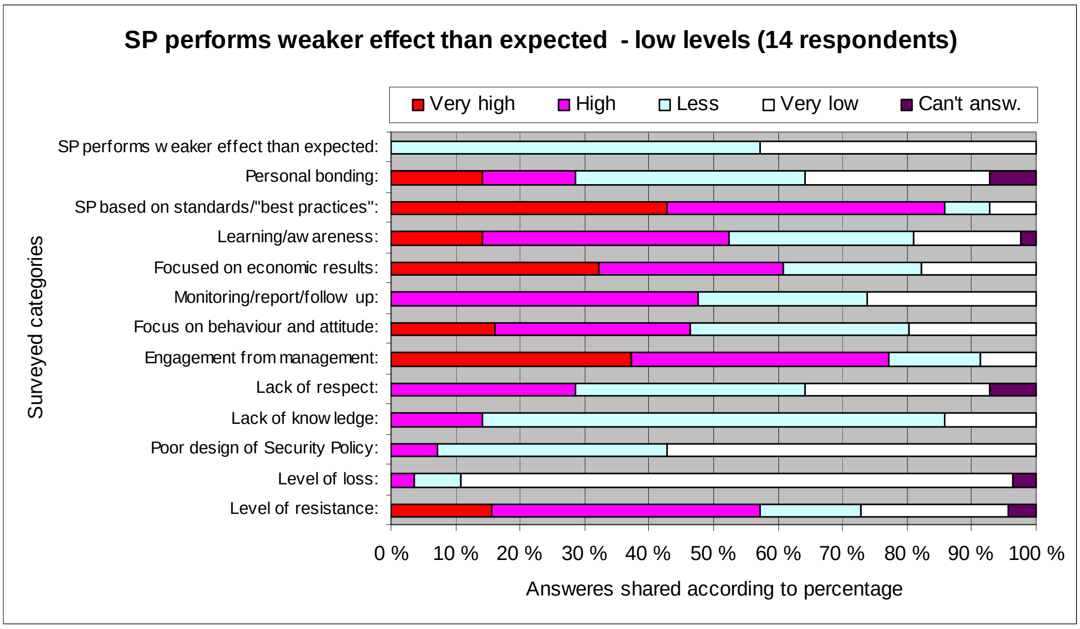


Table 4-10. Diagram "SP performs weaker effect than expected" (low levels)

The statistical material is still very sparse and unbalanced with eight respondents compared to fourteen. (Two respondents with "can't answer" give twenty-four).

4.2.3 Examining parameter: "Monitoring use and effect of the SP"

Looking at whom of the respondents that have arrangement for following up the security policy "Monitoring use and success of the SP", we find seven respondents. Related to the question about "effect" of the security policy is it reason to believe that those respondents "Monitoring use and effect of the SP" responds answers with higher reliability and validity than the respondents not having such arrangement in place.

Looking at the differences between "high" and "low" level respondents, following differences reveal.

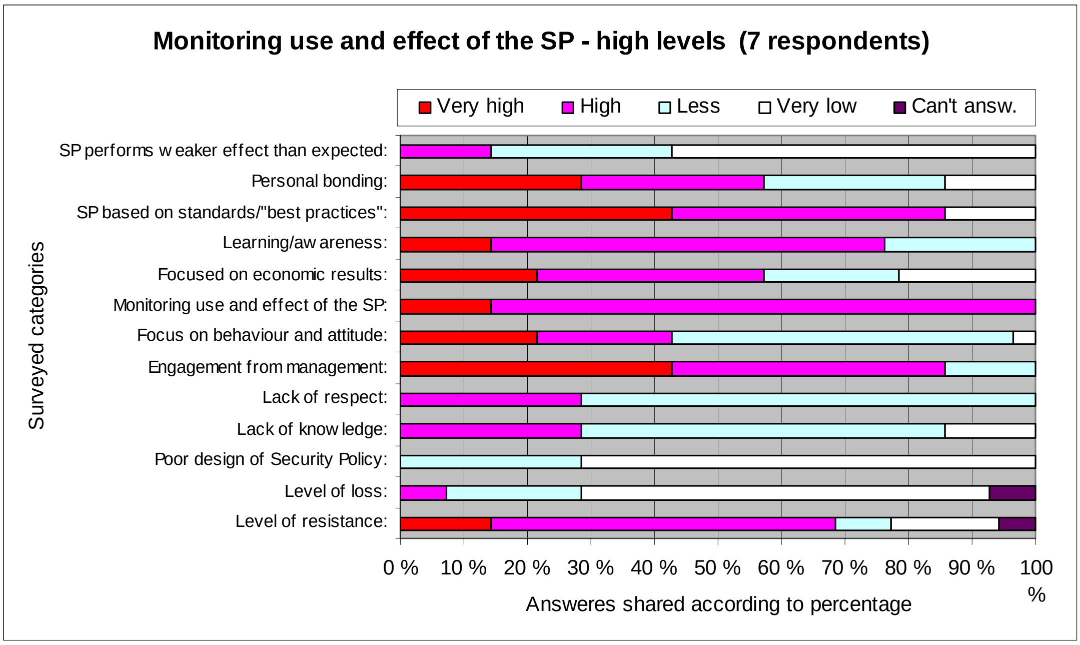


Table 4-11. Diagram "Monitoring use and effect of the SP" (high levels)

We see that the results support the findings from the entire group regarding "Engagement from management" and "Learning/awareness".

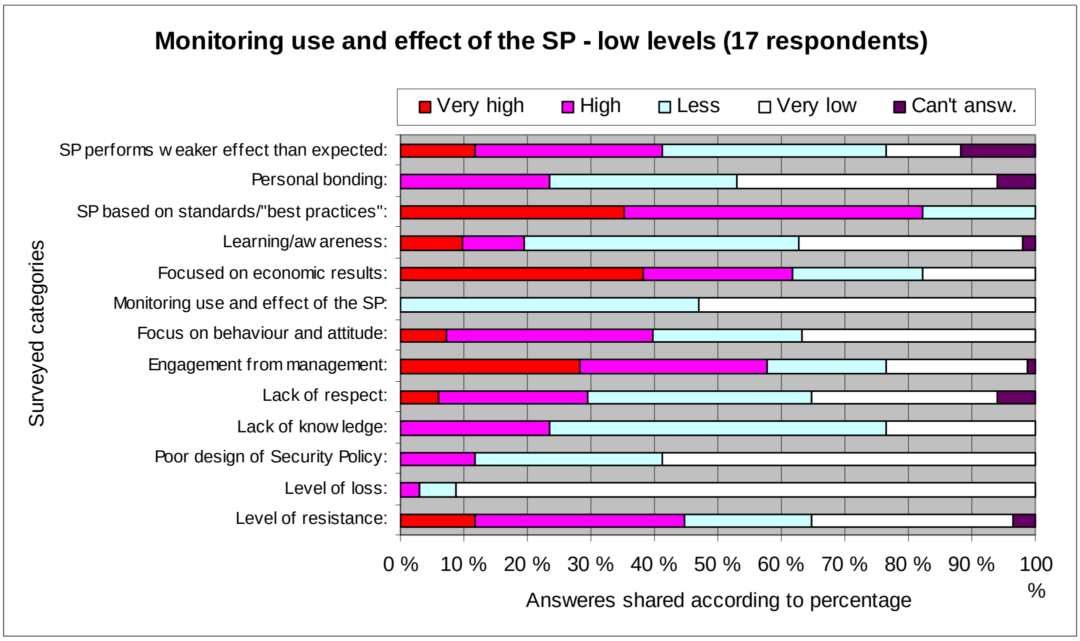


Table 4-12. Diagram "Monitoring use and effect of the SP" (low levels)

What is also of interest to notice is that "Level of resistance" is expressive higher in this group and also the parameter "Personal bonding".

"Level of loss" also shows higher figures even taking the component "can't answer" into consideration.

It is remarkable to notice that that six of the respondents are located in the group of the fourteen, which answered "security policy not weaker than expected". The seventh, which answered "Very high", is however located in the "SP weaker group".

Those six gains expected "effect" from the security policy. The response indicates a very good control with tight arrangement showing that they are following up the security policy.

Those six also reports that the policy is well integrated in the working processes (see table 4-13), and that it is conformity between the security policy and practice.

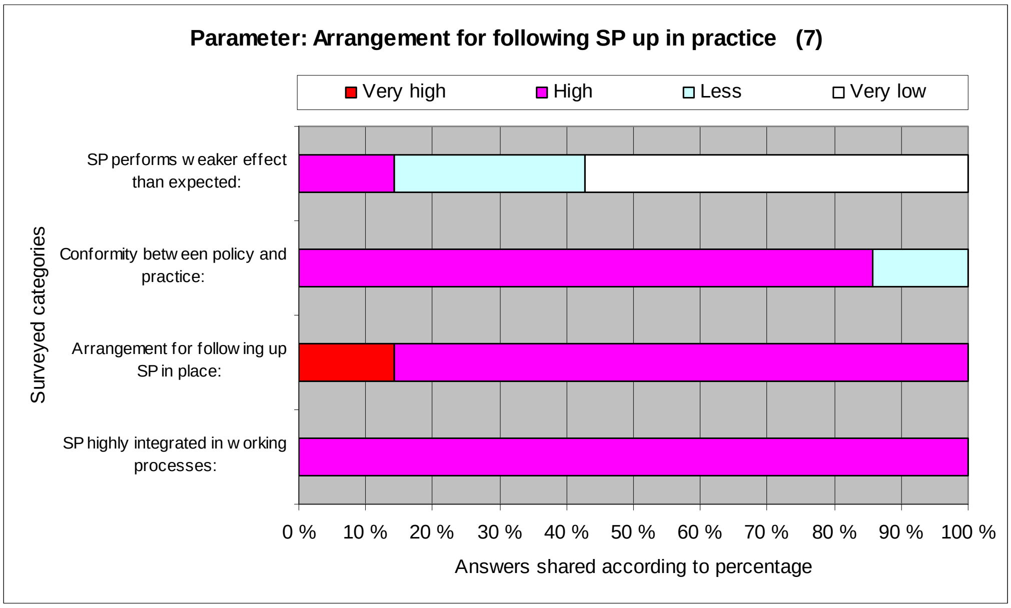


Table 4-13. Diagram **"**Arrangement for following security policy up in practice"

However, security breaches related to "Lack of respect" is still standing with 29%.

4.3 Examining parameters related to “Level of resistance”

This parameter is made up of elements considered to be of high importance in the aim of gaining “good health” or “robustness” against present and potential threats. The parameter is as discussed in chapter 3.3.4 one approach to what “Level of resistance” could possibly be.

4.3.1 Respondents reporting “high values” on “Level of resistance”

We start with respondents reporting high values on “Level of resistance”. This parameter embraces five questions and it is reasonable to believe that few respondents scores “High” on all of them. However, we found three respondents reporting “Very high” and “High”. In addition, we found two respondents that accommodate four out of five questions. These two reported negative on the question “Certified in accordance to a security standard”.

Level of resistance:		Very high	High	Less	Very low	Can't answ.
		6	17	0	1	1
We have arrangement for preparedness, crisis- and contingency management, which is tested yearly.	5	1	4	0	0	0
We are working a lot in purpose to determine adequate security measures in our organization.	5	1	4	0	0	0
The objectives/directives stated in the Security Policy is highly integrated in the organizations working processes.	5	0	5	0	0	0
Is the organization certified in accordance with an security standard? [*]	5	3	0	0	1	1
Our organization has defined a "security baseline" for system-technical security measures.	5	1	4	0	0	0

Table 4-14. Results **“**Level of resistance” (high values)

The security policy is based on standards/”best practises” for all respondents.

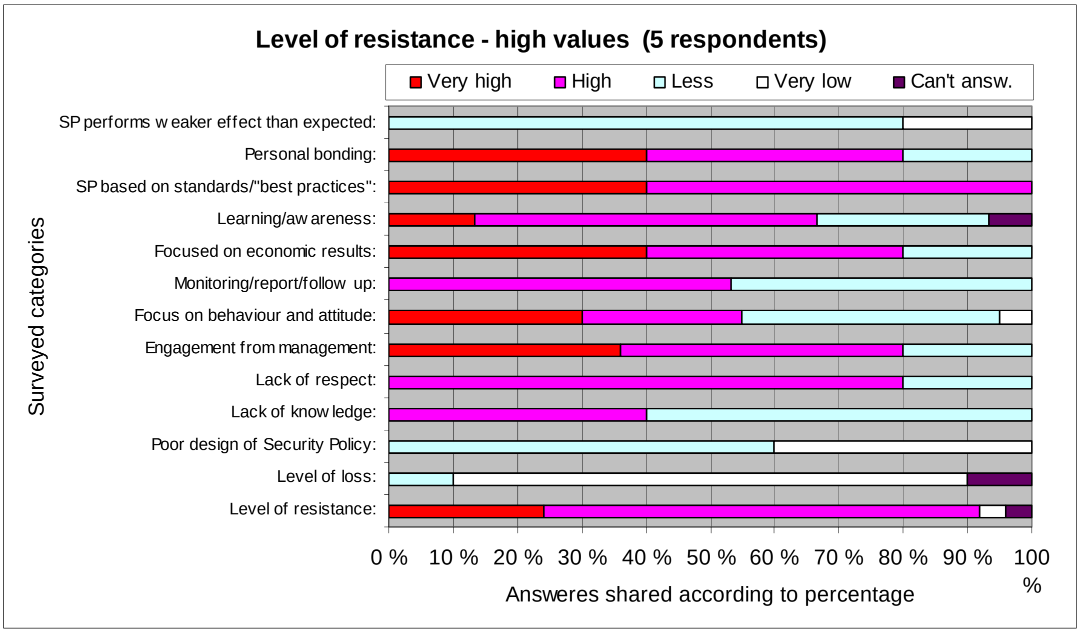


Table 4-15. Diagram “Level of resistance” (high values)

What is of interest to reflect on is that all of the respondents in this “class” reports that the security policy gains about expected “effect”.

SP performs weaker effect than expected:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**4**	**1**	**0**
Has the security policy weaker effect than expected in your organization?	5	0	0	4	1	0

Table 4-16. Results **“**SP perform expected effect” (“Level of resistance” high values)

“Engagement from management” gains a very good score with a total on 80% represented by 36% “Very high” and supported with 44% “High”.

Engagement from management:	36 %	44 %	20 %	0 %	0 %

Table 4-17. Results “Engagement from management” (“Level of resistance” high values)

No economical loss is reported.

Level of loss:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**1**	**8**	**1**
Has your organization realised an essential economical loss due to security breaches caused by own employees (insiders) last year?	5	0	0	1	3	1
Has your organization realised an essential economical loss due to security breaches caused by external unauthorized threats last year?	5	0	0	0	5	0

Table 4-18. Results “Level of loss” (“Level of resistance” high values)

“Poor design of security policy” does not seem to be a problem. “Lack of knowledge” is reported to be a bigger problem as a cause to security breaches and supports previous finding.

However, a remarkable finding is that “Lack of respect” is reported “High” (ref. table 4-15 and 4-19).

Lack of respect:		Very high	High	Less	Very low	Can't answ.
		0	**4**	**1**	**0**	**0**
In what extent are security breaches traceable due to employees lack of respect for the security policy?	5	0	4	1	0	0

Table 4-19. Results “Lack of respect” (“Level of resistance” high values)

This finding is remarkable due to the overall effort in security work reported from those respondents.

It still seems that the security policy does not aim to establish “respect” among the employees and is an important cause to security breaches.

The overall picture show high robustness and it is reason to believe that these organizations are fit for fight due to impact from potential threats.

The control question whether there is conformity between what is written in the security policy and practical experience is confirmed by four of the respondents. One respondent reports “Less”.

Conformity between policy and practice:		Very high	High	Less	Very low	Can't answ.
		0	**4**	**1**	**0**	**0**
Do you experience conformity between what is written in the security policy and practical experience in your organization?	5	0	4	1	0	0

Table 4-20. Results "Conformity between SP and practice" ("Level of resistance" high values)

4.3.2 Respondents reporting "low values" on "Level of resistance"

It is of interest to look at the contrary end regarding "Level of resistance". The respondents answering "Less" and "Very low" on the questions related to "Level of resistance" were selected.

Level of resistance:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**5**	**15**	**0**
We have arrangement for preparedness, crisis- and contingency management, which is tested yearly.	4	0	0	1	3	0
We are working a lot in purpose to determine adequate security measures in our organization.	4	0	0	1	3	0
The objectives/directives stated in the Security Policy is highly integrated in the organizations working processes.	4	0	0	2	2	0
Is the organization certified in accordance with an security standard? [*]	4	0	0	0	4	0
Our organization has defined a "security baseline" for system-technical security measures.	4	0	0	1	3	0

Table 4-21. Results "Level of resistance" (low values)

Four respondents were found showing another picture than the previous one.

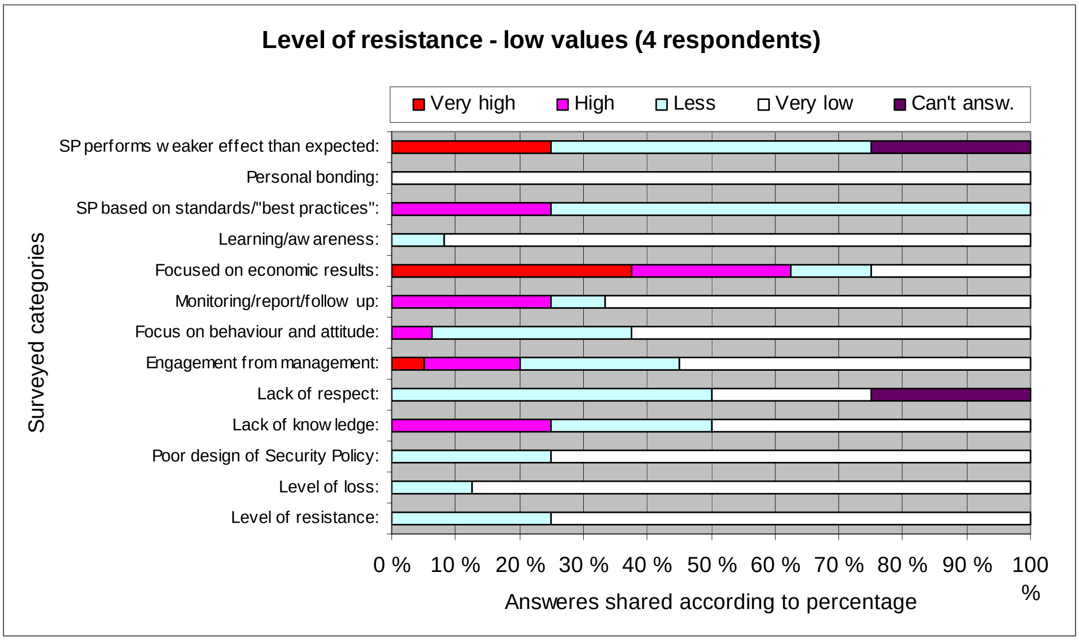


Table 4-22. Diagram **"**Level of resistance" (low values)

Looking at table 4-22 the results shows low values on:

- Engagement from management
- Learning/awareness
- Focus on behaviour and attitude
- Personal bonding
- SP based on standards/”best practices”

Level of “Lack of knowledge” due to lack of effort on “Learning/awareness” was expected higher. However, the numbers of respondents do not stand for statistical analysis.

One respondent reports “Very high” on “security policy weaker than expected”.

The control question whether conformity between security policy and practice, is responded with low values.

Conformity between policy and practice:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**3**	**1**	**0**
Do you experience conformity between what is written in the security policy and practical experience in your organization	4	0	0	3	1	0

Table 4-23. Results “Conformity between policy and practice” (“Level of resistance” low values)

Security breaches due to “Lack of respect” are however reported low and with a component of “Can’t answer.”.

However, what is of interest to observe is that reported “Level of loss” is about equal with organizations reporting, high values on “Level of resistance”.

It is interesting that “Measuring/reporting/follow up ICT systems” is equal with the previous respondents. Monitoring systems is of vital importance to keep control with what is “going on”.

Monitoring/report/follow up:		Very high	High	Less	Very low	Can't answ.
		0	**3**	**1**	**0**	**0**
Has the organization adequate routines for measuring, reporting and following up of faults/incidents in the ICT systems?	4	0	3	1	0	0

Table 4-24. Results **“**Monitoring/report/follow up” (“Level of resistance” low values)

Two out of three respondents reported no obligations related to legislation and directives. This may be an indication that official interventions help hence to emphasize security work.

Two out of four respondents keep updated from external sources about what could be actual/potential threats.

Use of external sources to keep update on present/potensial threats		Very high	High	Less	Very less	Can't answ.
		0	**2**	**1**	**1**	**0**
We use external sources to keep udated on what could be potensial threats to our organization	4	0	2	1	1	0

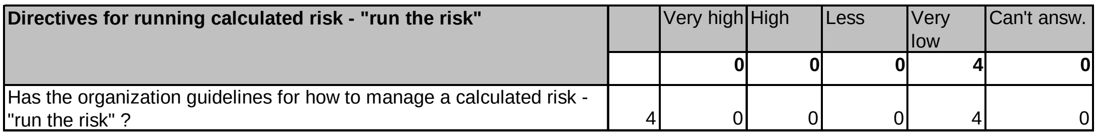
Table 4-25. Results “Updating present/potential threats” (“Level of resistance” low values)

Nevertheless, the results are an interesting observation due to readiness and the anticipated capability to withstand impact from insider threats and to recover from an accidental situation.

The respondents report that they focus on economical results and it is reason to believe that economical loss can be considerable if threats occur.

The result could be acceptable under the condition that management has decided to “run the risk”.

However, one of the questions in the questionnaire was whether the organization had guidelines for “run the risk”. In this case, all responds “Very low”.



Directives for running calculated risk - "run the risk"		Very high	High	Less	Very low	Can't answ.
		0	**0**	**0**	**4**	**0**
Has the organization guidelines for how to manage a calculated risk - "run the risk" ?	4	0	0	0	4	0

Table 4-26. Results “Directives "run the risk"” (“Level of resistance” low values)

4.4 Examining parameters related to "economical objectives"

The questionnaire contained questions in what extent the respondent organizations focused on economical results. Sixteen of the respondents answer that they focus on economical results and eight that they do not.

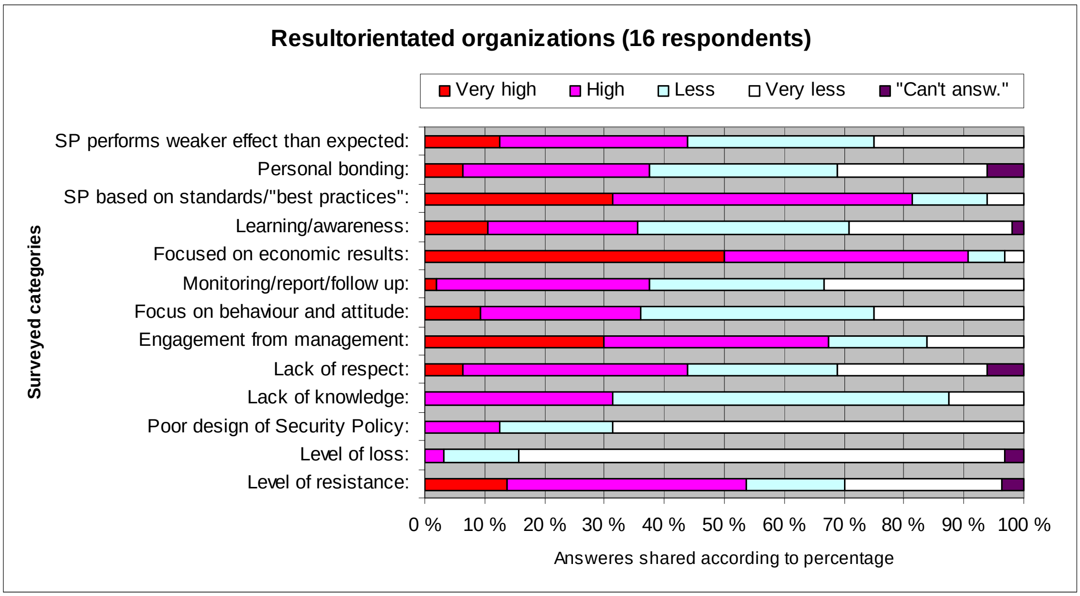


Table 4-27. Diagram **"**Result oriented organizations"

The answers indicate some differences between result-oriented and not result-oriented organizations.

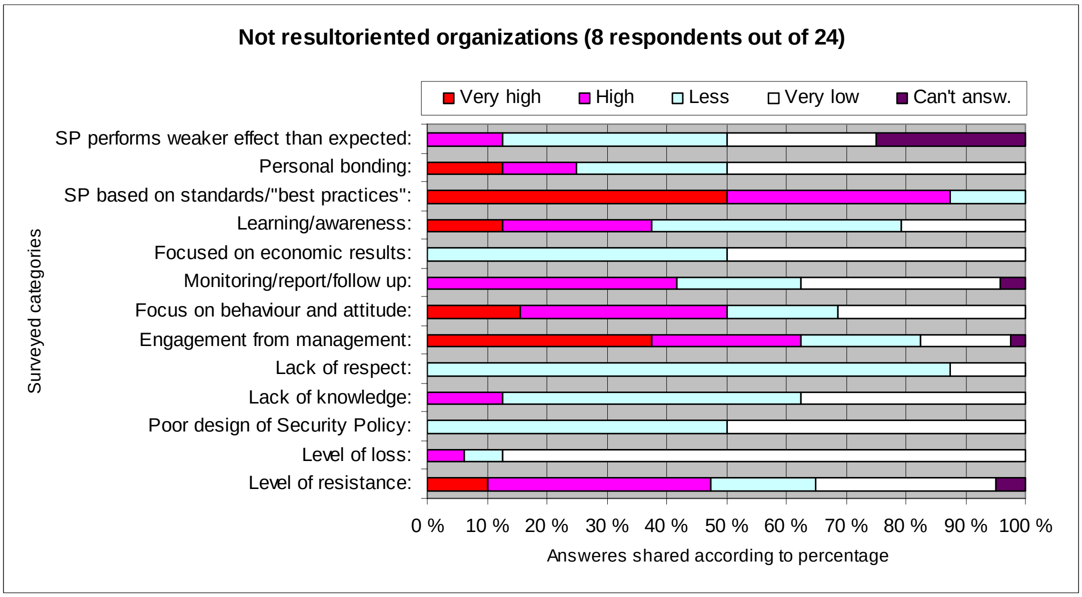


Table 4-28. Diagram **"**Not result-oriented organizations"

Focused on economic results:		Very high	High	Less	Very low	Can't answ.
		16	**13**	**2**	**1**	**0**
Is the organization that you are working in focused on economical objectives and results?	16	9	7	0	0	0
In our organization many of the employees are evalutated against economical results.	16	7	6	2	1	0

Table 4-29. Results "Focused on economical results" (result-oriented organizations)

About "effect" from the policy the result-oriented organizations reports "weaker effect" from the policy than the not result-oriented organizations. The answers are however accompanied with two respondents reporting, "can't answer" from the not result-oriented group. The materiel is considered to unbalanced to support any indication.

SP performs weaker effect than expected	0 %	13 %	38 %	25 %	25 %

SP performs weaker effect than expected		Very high	High	Less	Very low	Can't answ.
		0	**1**	**3**	**2**	**2**
Has the security policy weaker effect than expected in your organization?	8	0	1	3	2	2

Table 4-30. Results "SP performs weaker effect than expected" (not result-oriented organisations)

About "Level of resistance", the reported figures show very little difference between the two groups.

However, an interesting finding is the reported figures related to "Lack of Respect". In not result-oriented organizations all respondent's reports that security breaches related to "Lack of respect" to be "Very low".

Lack of respect:	0 %	0 %	88 %	13 %	0 %

Lack of respect:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**7**	**1**	**0**
In what extent are security breaches traceable due to employees lack of respect for the security policy?	8	0	0	7	1	0

Table 4-31. Results "Lack of respect" (organizations not focused on economical objectives)

The result-oriented organizations report seven respondents with high values. Only four out of the sixteen respondents reports "Very low". This is a significant difference to be aware of.

Lack of respect:	6 %	38 %	25 %	25 %	6 %

Lack of respect:		Very high	High	Less	Very low	Can't answ.
		1	**6**	**4**	**4**	**1**
In what extent are security breaches traceable due to employees lack of respect for the security policy?	16	1	6	4	4	1

Table 4-32. Results "Lack of respect" (organizations focused on economical objectives)

This is an interesting finding due the overall feedback on the parameter "Lack of respect". The other causes to security breaches "Poor design" and "Lack of knowledge" are also reported lower than the values in the result-oriented group.

5 ANALYSIS

All that is comes from the mind; it is based on the mind, it is fashioned by the mind
-The Pali Canon

5.1.1 Accumulated results all respondents

The method approach used in the chapter 4, “Findings” was to look for “differences” in the reported material related to our definition of “effect”. In cases “differences” appeared within the population, the differing parameters were noticed. The findings are analysed in this chapter.

Looking at the organisations overall, the accumulated results must be considered as good. This result was also anticipated from the selection of respondents done.

The “can’t answer” alternative (answered with 4% or higher) is considered important as a reflection due to which of the factors that was problematic to answer.

The questions related to “effect” and the parameters “Lack of respect” and “Personal bonding” gains the highest score and may serve as an indicator to what could be the challenges.

5.1.2 “Effect” of the security policy and it’s key factors

The security policy is reported to gain weaker “effect” than expected from 1/3 of the organizations. A figure of this size gives support for our suspicion that the work with security policies does not gain appropriate “effect” in a relatively high number of organizations concerned.

Compared with the respondents reporting “effect as expected” these respondents show considerably lower figures on the following parameters:

- Engagement from management
- Learning/awareness

Those respondents reporting “weaker effect than expected” also reports higher figures on the three questions regarding “causes to security breaches related to the SP”. Especially the question related to:

- Lack of knowledge

is significant higher. This makes sense due to the relationship between “Learning/awareness” and “Lack of knowledge”.

Examination of respondents performing “Monitoring use and success of the SP” support the findings done in the entire population. In addition, those respondents disclosed better values on the parameters:

- Level of resistance
- Personal bonding

Those respondents’ gains “expected effect” from the security policy. The policy is also well integrated in the working processes. Implicit, this group reflects focus on attainable security objectives involving the working processes due to the high score related to robustness represented by “Level of resistance”.

This reflection support the literature arguing that levels and structure assists effectiveness and efficiency in the way that the high-level policy focuses on the security objectives (doing the right things) and that the lower level policies focus on efficiency (doing things right).

It is reasonable to anticipate that the “high-level” respondents posses’ better “health” due to robustness than the “low-level” groups and are less vulnerable due to operational problems caused by poor security.

The parameter “Monitoring use and effect of the SP” seems to gain very good “effect” and support the use of a “security metrics program”. The results indicate that knowledge about what is “going on” leads to a higher level of focus and control and the preferred situation “measured and managed”.

The parameters that appear as key factors related to the security policy are:

- Engagement from management
- Learning/awareness
- Personal bonding
- Monitoring, measuring, following up
- Focus attainable security objectives involving the working processes

5.1.3 ”Level of resistance” and it’s key factors

It is of interest to notice that it is considerable differences in the security parameters between the organizations reporting “high” and “low” on “Level of resistance”. Respondents reporting high values on “Level of resistance” perform significantly better on the parameters:

- Engagement from management,
- Cultural aspects (behaviour/attitude)
- Learning (awareness)
- Personal bonding
- Measuring, reporting, follow up

Even taken the suppositions described in chapter 3.3.7, reliability and validity in consideration, the results indicates, that “human related” parameters are significantly more pronounced in organizations reporting high levels on “Level of resistance”.

These findings support the literature that human related parameters are of importance in making security success within an organization.

The differences in “high” and “low” level groups related to “effect” are interesting due to readiness and the anticipated capability to withstand impact from potential threats and to recover from an accidental situation as indicated in the previous chapter.

Due to the survey [NSO 2001] “Mørketallsundersøkelsen 2001”,[15] it is reported very high dependency of IT-systems. 80% of the respondents reports that they will approach severe problems already the first day the systems is out of operation.

The results observed in the “low-level” groups are also interesting in reflection of the management attitude accepting risk. As discussed, security is about economy and a matter of balancing risks. The result could be acceptable under the condition that management has decided to “run the risk”.

As referred in chapter 4.2.2 one of the questions in the questionnaire was whether the “low-level” organizations possess guidelines for “run the risk”. In this case, all responded “Very low”.

If the security level is not appropriate with the management’s point of view about “run the risk”, it is of importance to mind the gap. The management maintains responsibility for balancing the risks taken.

Even the respondents with low-values related to robustness should be in hold of premium technical security procedures and mechanisms, the insider problem no matter how is present as potential problem. This due to security breaches, caused either by unintended incidents or by deliberate acts.

It has to be concluded that the security policy in the “low-level” organizations do not offer adequate “effect” and the reason for this most likely is a subset of factors. Anticipated factors are “shortcomings” related to focusing security objectives and less focus on the “human factors”.

The parameters that appear as key factors related to robustness (“Level of resistance”) are:

- Engagement from management
- Learning/awareness
- Personal bonding
- Monitoring, reporting, following up
- Cultural aspects (behaviour/attitude)

The parameters are equal with the parameters for “effect” from the security policy except for one:

- Cultural aspects (behaviour/attitude)

This is reasonable due to the anticipated focus on security objectives on a long term basis.

[15] A new survey is released June this year. Figures have not been available in time for this work.

5.1.4 "Level of loss" as parameter for measuring "effect"

As mentioned economical loss due to security breaches is at "the end" the parameter that governs the security effort. Serious incidents will most likely affect the enterprise economy indicating to what extent a security policy is effective.

The respondents overall reports:

- Low economical losses.

The question in what extent the respondent's holds adequate systems for measuring loss is of due interest, but was not asked for in the survey.[16]

The parameter "Level of loss" is considered somewhat diffuse due to the elements direct and indirect losses. Indirect economical losses related to security breaches most likely represent the highest losses due to problems with availability and recovering from incidents.

It is anyway of interest to notice that it is less difference regarding "Level of loss" between the "high" and "low" level groups hence to reported "effect" from the policy and "Level of resistance".

These findings are not in accordance with the often shown figure, showing correspondence between resources used for security measures and mutually decrease in cost related to security breaches. The illustration (figure 5-1) is captured from [Daler, Gulbrandsen, Høie, Melgård, Sjølstad 2002] *p.35*

Use of economical loss as a parameter for measuring "effect" of the security policy is in this work considered not appropriate.

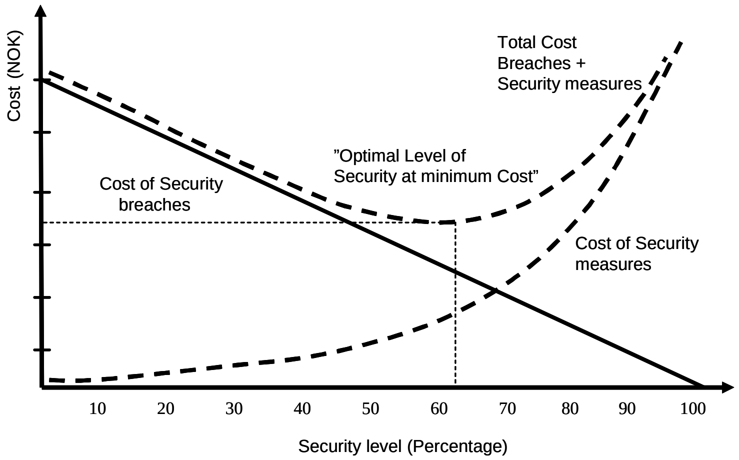


Figure 5-1. Optimal level of security at minimum cost

[16] Use of measurement systems e.g. use of metrics is in this case considered to be of interest for further examination.

5.1.5 Causes to security breaches

Our objective is to reveal characteristics due to the security policy that most likely leads to security breaches and hence influence the "effect" obtained from it.

The findings points at the surroundings and that the human related parameters we have emphasized in our questionnaire are of importance.

Findings of interest are that:

- It is a common agreement among the respondents that most of the security breaches can be looked upon as unintended incidents perceived as faults and accidents caused by human error.

- The security officer does not experience that "outline of the security policy" is the cause of security breaches to any extent.

- "Lack of knowledge" is a problem.

- "Lack of respect" is reported a greater problem than "Lack of knowledge". "Lack of respect" is reported to be a considerable problem in all circumstances except for organizations "not focused on economical objectives".

The survey has revealed that making a security policy effective the policy itself (design, outline, how communicated) seems to be off less importance. A majority of the respondents use standards or "best practices" in preparation of the policies. Within the scope of security maturity, this is edifying and to some extent expected based on the criteria companies were chosen on.

Having in mind our findings from the literature study, this is necessarily not comforting. The standards attempt to describe the various processes and controls needed for successfully implementing an information security policy. Less focus is emphasized on issues that most likely play an equal role of importance regarding security, the human factors.

Lack of knowledge is considered being a problem and points at the parameter learning/ awareness issue.

The implementation of effective security controls is dependent upon creating a security positive environment where employees understand and engage in the behaviour that is expected of them. The use of security awareness to create and maintain security-positive behaviour is a critical element in an effective information security environment.

Without a clear and communicated policy, it can be difficult to take action against staff who misuses corporate systems.

> "Human error rather than flawed technology is the root cause of most security breaches. Therefore, the challenge for many organisations is to create a security-aware culture. Making staff aware of the risks and their responsibilities help, them act in a sensible and secure manner." [ISBS 2004] *p.8*

This is a management issue and the management responsibility to assure being taken care of.

Johnny Mathisen deals with the awareness question in his MSc.thesis, “Measuring information security awareness”. [Mathisen 2004].

The throughout finding related to “Lack of respect” is however a sign to be aware of. Lack of respect for the security policy is a very less comfortable situation related to the finding that most of the security breaches can be looked upon as unintended incidents perceived as faults and accidents caused by human error.

However, an interesting finding is the reported figures related to “respect” in not result-oriented organizations. The respondent’s reports that security breaches related to “Lack of respect” are very low compared with the result-oriented ones.

The condition “respect” seems to be an issue related to “economical objectives” and hence corresponding culture.

6 CONCLUSION

The thesis work has shown that making an effective security policy is an embracing task. In definition of effective, literature points at effectiveness and efficiency. Effectiveness as focusing on the right things (objectives) and specify the objectives in a way that can be accomplished. Efficiency is concerned with “doing things right”. The intention with the security policy is to establish an organizational environment resistant to present and potential threats.

Writing an effective information security policy requires knowledge and experience in having full understanding of the organizational objectives and its particular strengths and weaknesses.

The first step of interest to investigate was to find out what “effect” the security policy produce within a certain environment. This was carried out by use of a questionnaire with intention to disclose parameters most likely influencing the produced “effect”.

Looking at the entire population of responding organizations, the accumulated results as an average must be considered as good. This result was also anticipated from the selection of respondents done.

It was found considerable differences in the security parameters between the organizations reporting “high” and “low” values on “effect” related to the security policy and organizational robustness.

Respondents’ reporting high values performs significantly better on the parameters:

- Engagement from management,
- Cultural aspects (behaviour/attitude)
- Learning/awareness
- Personal bonding
- Measuring, reporting, following up
- Focus on attainable security objectives involving the working processes

It is a common agreement among the respondents that most of the security breaches can be looked upon as unintended incidents perceived as faults and accidents and that most likely is caused by human error. This assumption is important to be aware of related to the work with the security policy and its most pronounced causes to security breaches.

Three causes to security breaches related to the policy were examined. The findings indicate that design of the policy is the least significant cause. It is a considerable difference between the values reported related to “Poor design” and the higher values reported related to “Lack of knowledge” and “Lack of respect” of the policy.

The throughout finding related to “lack of respect” is however a sign to be aware of. Lack of respect for the security policy is a very less comfortable situation related to the finding that most of the security breaches could be looked upon as unintended incidents perceived as faults and accidents caused by human error.

The issue “respect” seems to be a condition related to economical objectives and hence corresponding culture. What the reason could be is not given from the survey. It is considered to be of high interest to understand mechanisms related to respect.

Organizations that perform “Monitoring use and effect of the SP” on either organization level, or related to security policies gain higher scores on “effect”. A majority of those respondents makes use of defined goals (use “security baseline”) and has integrated security activities well in the working processes.

The results indicate that monitoring and measuring the “environment” in question leads to a higher level of focus and control, and the preferred situation “measured and managed”.

All work concludes that the human side of enterprise – people is important. It is crucial to the effectiveness and success of the security work that the security policy describes attainable security objectives involving the working processes.

The findings support the literature arguing that levels and structure assists effectiveness and efficiency in the way that the high-level policy focus on the security objectives (doing the right things) and that the lower level policies focus on efficiency (doing things right).

The implementation of effective security controls is dependent upon creating a security positive environment where employees understand and engage in the behaviour that is expected of them. The use of security awareness to create and maintain security-positive behaviour is a critical element in an effective information security environment.

“Engagement from management” is inevitably reported as an important factor in achieving appropriate framework in the aim of making security policies effective.

The parameters examined and that appear to be key factors related in making information security policies effective are:

- Engagement from management
- Learning/awareness
- Personal bonding
- Monitoring, reporting, following up
- Cultural aspects (behaviour/attitude)
- Focus attainable security objectives involving the working processes

The high-level corporate policy is obvious important in the light of its duty to tie objectives and principles together, and orchestra all activity hence to information security in the organization.

7 FURTHER WORK

The work with security policies and questions related to “effect” has been highly interesting and it is recommended to whom interested in this field to gain more knowledge about factors influencing “effect”. With reference to chapter 2.6 “Less research on the subject”, I hope that this work initiate motivation for other student’s works in reaching a higher level of comprehension.

However, the expected challenge in gaining information within this field has to some extent proved to be an issue.

This thesis has looked upon the topic from a holistic view and it should be good possibilities to focus severe areas discussed and examine these in more detail. It could be of interest to approach this topic from another angle of research. With the knowledge from this work, it could have been an issue to segment the topic into smaller areas and examine those with use of qualitative methods.

The underlying policies are only discussed in the extent of understanding the role to the corporate policy and may be subjects for further work with policies. Knowledge about these policies and the question related to their efficiency should be an issue of highly interest.

8 BIBLIOGRAPHY

8.1 Literature

[Creswell 2003] John W. Creswell, Research Design: Qualititative,quantitative, and mixed methods approaches, 2nd ed.(Sage Publications, CA, USA, 2003), ISBN 0-7619-2441-6........... 3

[Daler, Gulbrandsen, Høie, Melgård, Sjølstad 2002] Torgeir Daler, Roar Gulbrandsen, Tore Audun Høie, Birger Melgård, Torbjørn Sjølstad, Håndbok i datasikkerhet- informasjonsteknologi og risikostyring, (Tapir Akademisk Forlag, Trondheim 2002), ISBN 82-519-1785-9 18; 51

[Denscombe 2003] Martyn Denscombe, The good Research Guide for small-scale social research projects, Second edition (Open Univ. Press, PA, USA, 2003). ISBN 0 335 21303 0............ 24; 32

[Drucker 1973] Peter Drucker, Management: Tasks, Responsibilities, Practices, Harper&Row, 1973..... 14

[Fivelsdal, Bakka 1998] Egil Fivelsdal, Jørgen Frode Bakka, Organisasjonsteori: Struktur, kultur, prosesser, (Cappelen Akademisk forlag, Oslo 1998), ISBN 82-456-0099-7 18

[Grundy 1995] Tony Grundy, Breakthrough Strategies for Growth, (Pearson Education Ltd., England, 1995), ISBN 0-273-62046-0.. 4; 5

[Mathisen 2004] Johnny Mathisen, MSc.thesis, Measuring information security awareness, Gjøvik University College, June 2004. http://www.nislab.no.. 53

[Schein 1983] Edgar H. Shein, Organisasjonspsykologi, (Norsk utgave: Tanum-Norli A/S 1982,1983), ISBN 82-518-1614-9, Orginalens tittel: Organizational Psychology, 1980 by Addison-Wesley Publishing Company,Inc. 16

[Simonsen 2004] Geir Simonsen, MSc. thesis, “En prosess for sikkerhetsmetrikk program“ (A process for security metrics programs), Gjøvik University College, June 2004. http://www.nislab.no v

[Stamland 2004] Frank-Arne Stamland, MSc. thesis, Is BS7799 worth the effort, Gjøvik University College, June 2004. http://www.nislab.no.. 10

[Yngström 1996] Louise Yngström, A Systemic-Holistic Approach To Academic Programmes in IT Security, (Department of Computer and Systems Sciences, Stockholm University, 1996), ISBN 91-7153-521-7... 14

8.2 Digital Sources

[Adams & et.al 1997] A. Adams, M. A. Sasse, & P. Lunt, “Making passwords secure and usable”, People & Computers XII in proceedings of HCI’97 Springer 1997, A.Adams@cs.ucl.ac.uk.. 13

[Bennis 1962] Bennis, Toward a truly scientific management: The concept of organizational health. General Systems Yearbook, 1962 15

[Björck 2001] Fredrik Björck: Security Scandinavian Style, Interpreting the Practice of Managing Information Security in Organisations, DSV, Stockholm University / Royal Institute of Technology, 2001.Report series No. 01-017, ISSN 1101-8526, http://www.dsv.su.se. 12

[Booth, Colomb, Williams 2003] W. C. Booth, G.G. Colomb, J.M. Williams, The Craft of Research, 2nd ed., (The University of Chigago Press, USA, 2003), ISBN: 0-226-06567-5 2

[Brooke 2004] Paul Brooke, From the Top: Security Governance: Balancing Your Organization's Goals and Risk, Ensure well-directed security investments. Courtesy of American Financial Group, April 15, 2004, http://nwc.securitypipeline.com 1; 2

[BSI 2003] Bundesamt fur Sicherheit in der Informationstechnik, IT Baseline Protection Manual, October 2003, http://www.bsi.bund.de... 7

[Cavanagh 2002] James P. Cavanagh, Network Security: The Business Value Proposition, A White Paper for Management, January 2002, http://www.consultant-registry.com 11

[CESG 2002] CESG Common Criteria Certification in UK, UK IT security evaluaton and certification scheme, 2002.,http://www.cesg.gov.uk.. 7

[CIAO 2000] Critical Infrastructure Assurance Office, Practices for securing critical information assets, January 2000,Washington DC, http://www.infragard.net 7; 17

[Control Data 1999] Control Data Systems, Inc. White Paper, Why Security Policies Fail, Copyright 1999., http://downloads.securityfocus.com. 11; 12

[DTI 2003] The Department of Trade and Industry, UK, How to write an Information security policy, http://www.dti.gov.uk.. 7; 14

[Höne, Eloff 1/2002] Karin Höne and J. H. P. Eloff, What Makes an Effective Information Security Policy?, Network Security, Volume 2002, Issue 6, 1 June 2002, Pages 14-16, http://www.sciencedirect.com 1; 13

[Höne, Eloff 2/2002] Karin Höne and J. H. P. Eloff, Information security policy what do international information security standards say? Computers & Security 21(5) (2002) http://www.sciencedirect.com 8; 9; 11; 60

[ISBS 2004] PricewaterhouseCoopers and The department of Trade and Industry UK., Information security breaches survey 2004 (ISBS 2004), http://www.security-survey.gov.uk . 12; 34; 52

[ISF 2003] Information Security Forum (ISF), The Standard of Good Practice for Information Security, Version 4.0, March 2003, http://www.isfsecuritystandard.com..................................... 7

[Kormos & et.al 1999] Christina Kormos, Natalie Givans, Lisa A. Gallagher, Nadya Bartol, Using Security Metrics to Access Risk Management Capabilities, http://csrc.nist.gov 5

[Kotulic and Clark 2003] Andrew G. Kotulic and Jan Guynes Clark, Why there aren't more information security research studies, Information & Management, Volume 41, Issue 5, May 2004, Pages 597-607, http://www.sciencedirect.com... 20

[Kufås 2002] Ivar Kufås, Paper III, “A Framework for Information Security Culture”, Could it Help on Solving the Insider Problem?, December 2002, http://www.nsm.stat.no........... 5; 12; 20

[Mølmann 2003] Roy Are Mølmann, Paper II, “The Human Factor”, Taxonomy for classifying human challenges information security, May, 2003, http://www.nsm.stat.no 11

[Nielsen 2000] Fran Nielsen, Approaches to security metrics, A Report of the Workshop Held June 13-14, 2000 at the National Institute of Standards and Technology (NIST), http://csrc.nist.gov 19

[NIST 800-14] NIST, Special Publication SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, Semptember 1996, http://csrc.nist.gov...... 7

[NIST 800-55] NIST, Special Publication 800-55, Security Metrics Guide for Information Technology Systems, July 2003, http://csrc.nist.gov 19

[NSO 2001] Næringslivets sikkerhetsorganisasjon (NSO), Mørketallsundersøkelsen 2001, http://www.nso.no/index.htm 50

[NSW 1/2003] The New South Wales Department of Commerce, Australia Information Security Guideline for NSW Government – Part 3, Information Security Baseline Controls, Current version: June 2003, http://www.oit.nsw.gov.au 8

[NSW 2/2003] The New South Wales Department of Commerce, Australia, Information Security Guideline for NSW Government – Part 1 Information Security Risk Management, Current Version: Jun 2003, http://www.oit.nsw.gov.au 10

[RFC 2196] Network Working Group, Site Security Handbook, Request for Comments: 2196, Obsoletes: 1244 September 1997, Category: Informational, http://www.ietf.org......................... 4; 7

[ROSS 2003] Ivar Kufås & Roy Are Mølmann, Informasjonssikkerhet og innsideproblematikk, 2003-06-30.,ROSS (NTNU) 200301, ISBN 82-7706-204-4, http://www.nsm.stat.no 11

[Sumajit 2002] Rosemary Sumajit, Developing Security Policies: Charting an Obstacle Course,GSEC Version 1.3, April 4, 2002, http://www.sans.org.. 11; 14; 30

[Wies 1995] René Wies, Using a Classification of Management Policies for Policy Specification and Policy Transformation, Munich Management Team, University of Munich, Department of Computer Science, Munich, Germany, ... 17; 19

[Wills 2002] Laura Wills, Security Policies: Where to Begin. (December 12, 2002), http://www.sans.org v

[Wold 2003] Gullik Wold, MSc project plan, Is use of security metrics expedient to measure performance of an implemented organizational security policy?, HIG, Nislab, 2003, http://www.nislab.no v

[Wood 2000] Charles Cresson Wood, An unappreciated why information policies fail October 2000, Pages 13-14, Computer Fraud & Security, Volume 2000, Issue 10.,http://www.sciencedirect.com 12

[Yngstöm, Björck 2000] Fredrik Björck and Louise Yngström, A simple classification model for research in information security, IFIP World Computer Congress / SEC 2000 Revisited, http://www.dsv.su.se 20

9 APPENDICES

9.1 Appendices A: Elements of an information security policy

[Höne, Eloff 2/2002] *p.403-405*

ELEMENTS OF AN INFORMATION SECURITY POLICY

The elements of an information security policy focus on the different parts that make up such a document. The elements focus mainly on the overall content of the policy.

Need for and Scope of Information Security

This is a brief introductory statement emphasising the organisation's dependence on information and therefore information security. This introductory statement also provides the background as to why the policy is needed in the organisation.

Objectives of Information Security

The objectives of information security in an organisation should be described briefly to inform the reader of the specific aim of information security management in the organisation. These objectives should be clearly linked to the organisation's overall business strategy, goals and objectives and the nature of its business [OOIT01].

Definition of Information Security

An information security policy is generally targeted at a diverse audience for whom information security may be a foreign and new concept. It is therefore crucial that the policy contains a brief and understandable definition of information security to ensure a uniform understanding of the concept throughout the organisation.

Management Commitment to Information Security

The commitment statement is the singularly most important statement in an information security policy. Without this statement, any activities attempted by the information security personnel will not be effective and will not be taken seriously throughout the entire organisation [JISC01]. The management commitment statement can force employees to pay attention to information security and demonstrates management's intention of making a success of it in the organisation [WOOD95].

Approval of the Information Security Policy (Signature)

The approval signature can also be seen as the endorsing signature and should typically be that of the highest possible signatory in the organisation [OOIT01]. This signature should be displayed in a prominent position as a further sign of top management's commitment to information security.

Purpose or Objective of the Information Security Policy

The purpose or objective of the information security policy should not be confused with the introductory statements on the need for information security in an organisation. These statements rather describe the reasons for the development of an information security policy and will possibly be linked to legal compliance issues. The main goals of the policy itself are thus described in this section [JISC01].

Information Security Principles

The information security principles describe the general rules related to information security within an organisation. These principles try to explain to the users what is the correct and the incorrect behaviour in the organisation regarding various topics and concepts. Some of these principles will be closely linked to an organisation's culture or to regulatory requirements governing the industry in which the organisation is functioning. Others will, however, be applicable to all organisations and will be found in any information security policy, such as virus protection and user awareness and education. The principles will, however, also change over time depending on technological developments and changes. An information security policy written 20 years ago will generally make no reference to any form of electronic information security, but will probably make detailed reference to physical information security. It is therefore crucial that especially this part of the policy be regularly reviewed for applicability.

Roles and Responsibilities

This is one of the most important components of the information security policy, as this part tells the reader exactly what is expected of him/her in terms of information security in the organisation. The roles and responsibilities should cover all aspects of information security, as well as the individual responsibilities of all parties using the organisation's information resources [OOIT01].

Information Security Policy Violations and Disciplinary Action

The statement on information security policy violations is a very powerful statement, as it ensures that disciplinary action can be taken against a user if the policy is not adhered to. It is very important that this statement be directly related to the organisation's overall disciplinary policy.

Monitoring and Review

This statement deals with the need to frequently monitor and review the continued applicability and effectiveness of the information security controls implemented within the organisation [BSI00]. Without this statement there is no forced continuity for the improvement of information security implementation in the organisation.

User Declaration and Acknowledgement

This is not a common element found in an information security policy, and is usually presented as an appendix or a separate document. It is, however, a very useful element, as it is typically drafted as an abridged version of the information security policy and targeted completely at the users of the organisation. The users are then more likely to read the entire section and have a better understanding of what is expected from them. In signing a user declaration upon employment before access to electronic information is granted, the user acknowledges his/her responsibility with regard to information security. The user declaration and acknowledgement should also be read and signed again on an annual basis by all users to remind them of their individual responsibilities in protecting information assets within the organisation [TUDO01].

Cross References

The information security policy should never be written in isolation and will need to be supported by other relevant policies, standards, procedures and processes. These applicable documents should be referenced in the policy to ensure that the reader obtains a complete picture of all information security controls and measures used in the organisation. Often organisations are also required to implement certain controls and measures as determined by the country's legislation and regulations. These then also need to be referenced in the policy.

General Elements

Below is a brief list of further recommended elements to be included in an Information Security Policy to ensure its official status in an organisation. These elements are selfexplanatory and will only be listed below.

- The authors
- Date of the policy
- Review date of the policy

9.2 Appendices B: Cover letter

NISlab™
Norwegian Information Security laboratory

Gullik Wold
NISlab Norwegian Information Security laboratory [Nislab.no]
Gjøvik University College
2800 Gjøvik Mars-2004

Spørreundersøkelse informasjonssikkerhet

Mitt navn er Gullik Wold. Jeg har arbeidet med sikkerhet gjennom en god del år og har hatt mitt virke både innenfor privat og offentlig virksomhet (Forsvaret). Jeg er nå ansatt i ErgoIntegration AS som er et datterselskap av ErgoGroup AS, helheid av Posten Norge AS, hvor jeg arbeider med sikkerhet. Ved siden av arbeidet er jeg student ved Høgskolen i Gjøvik, Mastergradstudiet i Informasjonssikkerhet som ble opprettet høsten 2002. Studiet har vært svært lærerikt og interessant, og jeg er nå inne i siste semester og skriver en hovedoppgave med tittel: **What factors distinguishes an effective ICT security policy?** Veileder for oppgaven er Professor Einar Snekkenes.
.
Gjennom mange års virke innenfor fagområdet har jeg erfart at det er av største viktighet for en virksomhet å lage en sikkerhetspolicy som er forståelig, hensiktmessig og motiverer til bruk. Målet med denne hovedoppgaven er å finne frem til faktorer som kjennetegner en effektiv sikkerhetspolicy.

I arbeidet med å finne frem til dette gjennomfører jeg en spørreundersøkelse hos et antall store norske virksomheter. Henvendelsen går til virksomheter hvor behandling av elektronisk informasjon med bruk av Informasjon og Kommunikasjons Teknologi (IKT) anses å være en vesentlig faktor. Spørreundersøkelsen er lagt opp slik at avgitte svar er anonyme og virksomheten ikke sporbar.

Det sendes ut en konvolutt til deg som virksomhetens sikkerhetsansvarlig som inneholder et spørreskjema og som ønskes besvart av sikkerhetsansvarlig. Besvarelsen vil ta ca. 20-30 minutter.

Undersøkelsen sendes ut til 20 virksomheter og jeg har et håp om at så mange som mulig fyller ut skjemaet, legger det i vedlagte frankerte og adresserte konvolutt og legger det i en postkasse så raskt som mulig. Påskeuken er avsatt til resultatbehandling ☺.

Jeg håper din virksomhet har mulighet til å bistå i denne oppgaven. Dersom svaret er negativt, kastes det tilsendte materialet uten noen form for tilbakemelding.

Dersom du skulle være interessert i ta kontakt med meg, kan du kontakte meg på e-mail adresse: gullik.wold@ergo.no alternativt mob. tlf. 918 94 501.

Spørsmålene har fem svaralternativer. Fire av disse varierer fra Meget stor grad til Meget liten grad. Det er satt opp en brøk for å vise forholdet mellom disse og som ligger i intervallet mellom en og null. Dersom du er usikker eller ikke ønsker å svare på ett spørsmål, så bruk kolonnen ”Kan ikke svare”. Spørsmål hvor det er naturlig og svare Ja/Nei er kombinert med kolonnen ”Meget stor grad/Meget liten grad”.

På forhånd mange takk for hjelpen.

Med vennlig hilsen
Gullik Wold

9.3 Appendices C: Postal questionnaire

Spørreundersøkelse Sikkerhetspolicy: Fylles ut av sikkerhetsansvarlig	Svarkolonner				
Brøk viser gradsnivået mellom 1 og 0. Hvis Ja/Nei spm. kryss i ruten [1-3/4] for Ja. Nei i ruten [1/3-0]. Ja/Nei spm. er merket [*]	**Meget stor grad 1-3/4**	**Stor grad 3/4 -1/2**	**Mindre grad 1/2-1/3**	**Meget liten grad 1/3-0**	**Kan ikke svare**
Har virksomheten en Sikkerhetspolicy ? [*] (Med sikkerhetspolicy menes sikkerhetspolicy inklusive retningslinjer/prosedyrer, sikkerhetshåndbok etc.). Dersom svaret skulle være nei er det ønskelig at du besvarer de spørsmålene som fremdeles er relevante					
Trusselbilde:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Har din virksomhet hatt et vesentlig økonomisk tap som kan tilskrives sikkerhetshendelser forårsaket av egne ansatte siste året ?					
Har din virksomhet hatt et vesentlig økonomisk tap som kan tilskrives sikkerhetshendelser forårsaket av ekstern uautorisert aktivitet siste året ?					
Er du enig i påstanden om at de fleste sikkerhetshendelser skyldes utilsiktede handlinger som gjerne oppfattes som feil og uhell, og som i de fleste tilfeller kan tilskrives menneskelig svikt.					
Vi benytter oss av eksterne kilder for å holde oss oppdatert på hva som kan være aktuelle/potensielle trusler for vår virksomhet.					
Lover og direktiver:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Arbeider virksomheten med informasjon som er underlagt lovverk (forskrifter) som gir føringer for IKT systemer: Personopplysnings-loven, Kredittilsynets IKT forskrift, Forvaltningsloven etc. ?					
Sikkerhetspolicy nivå 1:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Er utarbeidelse av sikkerhetspolicy basert på standarder eller "best practices" (for eksempel ISF eller tilsvarende) ?					
Sikkerhetspolicy nivå 2:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Sikkerhetpolicyens totale størrelse i sider er; Meget stor: >100 sider, Stor: 99-60 sider, Mindre: 59-20 sider, Meget liten: < 19 sider					
Vår sikkerhetspolicy er inndelt i "emnebolker" med korte poengterte sammendrag.					
Sikkerhetspolicy utleveres virksomhetens medarbeidere i trykket utgave.[*]					
Vår sikkerhetspolicy er tilgjengelig via intranett. [*]					
Vår sikkerhetspolicy har illustrasjoner og/eller symboler som gjør innholdet lettere forståelig.					
Sikkerhetspolicyen har direktiv om at det skal finnes et undervisningsopplegg for sikkerhet.					
Direktivene/føringene i sikkerhetspolicyen er meget godt integrert i virksomhetens arbeidsprosesser.					
Ledelsens holdninger og prioriteringer:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Vår ledelse viser klart og tydelig i handling at sikkerhet er viktig for virksomheten					
Er virksomheten sertifisert iht. en sikkerhetsstandard [*]?					
Har du i løpet av siste året diskutert med dine kollegaer om hvordan dere kan gjøre sikkerhetspolicyen bedre ?					
Våre ansatte er den viktigste ressursen for å kunne oppnå god sikkerhet.					

Holdningsskapende arbeid:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Vår virksomhet er flinke til å orientere om hvilke holdninger og verdinormer virksomheten forventer av sine ansatte.					
Medarbeidere i vår virksomhet får opplæring i å forstå viktigheten av sikkerhet i forbindelse med eget arbeid.					
Gjennomføres det sikkerhetssamtaler med personell minimum en gang pr år ?					
Måling/rapportering /oppfølging:	**Meget stor grad 1-3/4**	**Stor grad 3/4 -1/2**	**Mindre grad 1/2-1/3**	**Meget liten grad 1/3-0**	**Kan ikke svare**
Har virksomheten gode rutiner for måling, rapportering og oppfølging av feilsituasjoner i IKT systemene?					
Vår virksomhet har definert en "security baseline" for systemtekniske sikkerhetstiltak.					
Blir ansatte målt på forhold relatert til sikkerhetspolicy (balanced scorecard, KPIer) ?					
Finnes det et opplegg for å etterprøve i hvilken grad sikkerhetspolicyen brukes og etterfølges ?					
Resultatorientering:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Er virksomheten du arbeider i økonomisk mål- og resultatorientert ?					
Vi arbeider mye med å finne frem til hva som er god nok sikkerhet i min virksomhet.					
Har virksomheten retningslinjer for hvordan man forholder seg til det å ta en kalkulert risiko - "run the risk" ?					
I vår virksomhet er det mange som blir målt på økonomiske resultater.					
Personlig nettverk - utveksling av informasjon:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Vi har et program med målsetting å få til kontrollert utveksling av sikkerhetsinformasjon på tvers av avdelinger/divisjoner.					
Vår virksomhet er avhengig av kunnskapen til "nøkkelpersoner".					
Læring:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Blir sikkerhetspolicyen gjennomått/ kurset jevnlig (minimum en gang pr. år) for de ansatte ?					
Budsjetteres "øremerkes" det midler til sikkerhetsopplæring ?					
Formidles det informasjon om sikkerhet via intranett ?					
Blir ansatte som arbeider med IKT basissystemer/infrastruktur trenet i å håndtere uforutsette sikkerhetshendelser ?					
Vi er kjent med, og orienterer virksomhetens ansatte jevnlig (månedlig) om sikkerhetstrusler og risiko relatert til virksomhetens arbeidsoppgaver.					
Sikkerhetsnivå:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Vi har et opplegg for beredskap, krise- og kontinuitets håndtering som testes minimum en gang pr. år.					
Opplever dere samsvar mellom det som står i sikkerhetspolicyen og det som skjer i praksis i din virksomhet.					
Sikkerhetshendelser relatert til Sikkerhetspolicy:	**Meget stor grad**	**Stor grad**	**Mindre grad**	**Meget liten grad**	**Kan ikke svare**
Har forhold som kan tilskrives mangelfull utforming av sikkerhetspolicy vært direkte årsak til sikkerhetshendelser i løpet av det siste året ?					
Har forhold som kan tilskrives ansattes manglende kjennskap til sikkerhetspolicy vært direkte årsak til sikkerhetshendelser i løpet av det siste året ?					
I hvilken grad kan sikkerhetshendelser spores tilbake til ansattes manglende repekt for sikkerhetspolicy ?					
Har sikkerhetspolicyen svakere effekt enn forventet i din virksomhet ?					

Resultater før/etter innføring av sikkerhetstiltak:	**Meget stor grad 1-3/4**	**Stor grad 3/4 -1/2**	**Mindre grad 1/2-1/3**	**Meget liten grad 1/3-0**	**Kan ikke svare**
Dersom virksomheten i løpet av de siste tre årene har hatt et konkret forbedringsprogram relatert til sikkerhetspolicy og har tallmateriale som viser situasjonen før og etter, spørres det om antallet sikkerhetshendelser har blitt vesentlig lavere.					
Dersom virksomheten i løpet av de siste tre årene har innført måling/hendelse/avvikssrapportering mhp. sikkerhet og har tallmateriale som viser situasjonen før og etter innføring, spørres det om antallet sikkerhetshendelser har blitt vesentlig lavere.					
Dersom virksomheten i løpet av de siste tre årene har igangsatt et konkret program for å øke sikkerhetsbevisshet og har tallmateriale som viser situasjonen før og etter innføring, spørres det om antallet sikkerhetshendelser har blitt lavere.					
Dersom virksomhetens ledelse har økt fokus/engasjement på sikkerhet og har tallmateriale som viser situasjonen før og etter innføring, spørres det om antallet sikkerhetshendelser har blitt vesentlig lavere.					
Demografi:	**Ja**	**Nei**			
Vår virksomhet har mer enn 100 ansatte.					

Takk for innsatsen :-)

Dersom du skulle ønske å kommentere/utdype noen av spørsmålene vil dette kunne være et verdifullt bidrag til løsning av oppgaven. Skriv gjerne på resten av dette arket.

9.4 Appendices D: Accumulated results all respondents

Result accumulated (24 respondents)						
Level of resistance:		Very high	High	Less	Very low	Can't answ.
		15	**47**	**20**	**33**	**5**
We have arrangement for preparedness, crisis- and contingency management, which is tested yearly.	24	4	11	5	4	0
We are working a lot in purpose to determine adequate security measures in our organization.	24	4	13	3	4	0
The objectives/directives stated in the Security Policy is highly integrated in the organizations working processes.	24	2	14	5	3	0
Is the organization certified in accordance with an security standard? [*]	24	3	0	0	19	2
Our organization has defined a "security baseline" for system-technical security measures.	24	2	9	7	3	3
Level of loss:		Very high	High	Less	Very low	Can't answ.
		0	**2**	**5**	**40**	**1**
Has your organization realised an essential economical loss due to security breaches caused by own employees (insiders) last year?	24	0	1	2	20	1
Has your organization realised an essential economical loss due to security breaches caused by external unauthorized threats last year?	24	0	1	3	20	0
Poor design of Security Policy:		Very high	High	Less	Very low	Can't answ.
		0	**2**	**7**	**15**	**0**
Have conditions due to poor design of the security policy been direct cause to security breaches during the last year?	24	0	2	7	15	0
Lack of knowledge:		Very high	High	Less	Very low	Can't answ.
		0	**6**	**13**	**5**	**0**
Have conditions due to lack of knowledge of the security policy been direct cause to security breaches during the last year?	24	0	6	13	5	0
Lack of respect:		Very high	High	Less	Very low	Can't answ.
		1	**6**	**11**	**5**	**1**
In what extent are security breaches traceable due to employees lack of respect for the security policy?	24	1	6	11	5	1
Engagement from management:		Very high	High	Less	Very low	Can't answ.
		39	**40**	**21**	**19**	**1**
Our management shows clear and explisit in action that security is important for the organization.	24	4	14	3	3	0
Have you during the last year discussed with your colleagues how to improve your security policy?	24	12	8	4	0	0
Our employees is the most important resources in the aim of acheiving adequate security.	24	17	5	1	1	0
The security policy directs that arrangement for teaching security shall be in place.	24	5	8	2	8	1
Do the budget assign resources for security education?	24	1	5	11	7	0

Focus on behaviour and attitude:		Very high	High	Less	Very low	Can't answ.
		11	**28**	**31**	**26**	**0**
Our organization is clever in communicating behaviour and attitude aspects anticipated from the employees.	24	2	14	4	4	0
We are known with, and communicates the employees regurlarly (monthly) about security threats and risks related to the organizational working tasks.	24	1	4	12	7	0
Is information about security communicated over the intranett?	24	7	9	7	1	0
Is security conversation with the employees accomplished at least one time during the year?	24	1	1	8	14	0
Monitoring/report/follow up:		Very high	High	Less	Very low	Can't answ.
		1	**27**	**19**	**24**	**1**
Has the organization adequate routines for measuring, reporting and following up of faults/incidents in the ICT systems?	24	0	21	3	0	0
Are the employees evaluated regarding performance related to the security policy (balanced scorecard, KPI's)?	24	0	0	8	15	1
Does it exist an arrangement for evaluating in what extent the security policy is used and succeeded?	24	1	6	8	9	0
Focused on economic results:		Very high	High	Less	Very low	Can't answ.
		16	**13**	**10**	**9**	**0**
Is the organization that you are working in focused on economical objectives and results?	24	9	7	6	2	0
In our organization many of the employees are evalutated against economical results.	24	7	6	4	7	0
Learning/awareness:		Very high	High	Less	Very low	Can't answ.
		8	**18**	**27**	**18**	**1**
Is the security policy communicated/teached the employees regurlarly (minimum one time a year)?	24	1	4	9	10	0
The employees in our organization are informed about understanding the importance of security issues related to their work.	24	4	8	8	4	0
Are employees working with ICT infrastructure trained in handling unforeseen security breaches?	24	3	6	10	4	1
SP based on standards/"best practices":		Very high	High	Less	Very low	Can't answ.
		9	**11**	**3**	**1**	**0**
Is preparation of the security policy based on standards or "best practices" (e.g. ISF or equivalents)?	24	9	11	3	1	0
Personal bonding:		Very high	High	Less	Very low	Can't answ.
		2	**6**	**7**	**8**	**1**
We have an arrangement with objective to exchange personal security knowledge between divisions/departments.	24	2	6	7	8	1
SP performs weaker effect than expected:		Very high	High	Less	Very low	Can't answ.
		2	**6**	**8**	**6**	**2**
Has the security policy weaker effect than expected in your organization?	24	2	6	8	6	2

9.5 Appendices E: High level of resistance

High level of resistance (5 respondents)						
Level of resistance:		Very high	High	Less	Very low	Can't answ.
		6	**17**	**0**	**1**	**1**
We have arrangement for preparedness, crisis- and contingency management, which is tested yearly.	5	1	4	0	0	0
We are working a lot in purpose to determine adequate security measures in our organization.	5	1	4	0	0	0
The objectives/directives stated in the Security Policy is highly integrated in the organizations working processes.	5	0	5	0	0	0
Is the organization certified in accordance with an security standard? [*]	5	3	0	0	1	1
Our organization has defined a "security baseline" for system-technical security measures.	5	1	4	0	0	0
Level of loss:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**1**	**8**	**1**
Has your organization realised an essential economical loss due to security breaches caused by own employees (insiders) last year?	5	0	0	1	3	1
Has your organization realised an essential economical loss due to security breaches caused by external unauthorized threats last year?	5	0	0	0	5	0
Poor design of Security Policy:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**3**	**2**	**0**
Have conditions due to poor design of the security policy been direct cause to security breaches during the last year?	5	0	0	3	2	0
Lack of knowledge:		Very high	High	Less	Very low	Can't answ.
		0	**2**	**3**	**0**	**0**
Have conditions due to lack of knowledge of the security policy been direct cause to security breaches during the last year?	5	0	2	3	0	0
Lack of respect:		Very high	High	Less	Very low	Can't answ.
		0	**4**	**1**	**0**	**0**
In what extent are security breaches traceable due to employees lack of respect for the security policy?	5	0	4	1	0	0
Engagement from management:		Very high	High	Less	Very low	Can't answ.
		9	**11**	**5**	**0**	**0**
Our management shows clear and explisit in action that security is important for the organization.	5	1	3	1	0	0
Have you during the last year discussed with your colleagues how to improve your security policy?	5	3	2	0	0	0
Our employees is the most important resources in the aim of acheiving adequate security.	5	4	1	0	0	0
The security policy directs that arrangement for teaching security shall be in place.	5	1	3	1	0	0
Do the budget assign resources for security education?	5	0	2	3	0	0

Focus on behaviour and attitude:		Very high	High	Less	Very low	Can't answ.
		6	**5**	**8**	**1**	**0**
Our organization is clever in communicating behaviour and attitude aspects anticipated from the employees.	5	2	2	1	0	0
We are known with, and communicates the employees regurlarly (monthly) about security threats and risks related to the organizational working tasks.	5	1	1	3	0	0
Is information about security communicated over the intranett?	5	3	1	1	0	0
Is security conversation with the employees accomplished at least one time during the year?	5	0	1	3	1	0
Monitoring/report/follow up:		Very high	High	Less	Very low	Can't answ.
		0	**8**	**7**	**0**	**0**
Has the organization adequate routines for measuring, reporting and following up of faults/incidents in the ICT systems?	5	0	5	0	0	0
Are the employees evaluated regarding performance related to the security policy (balanced scorecard, KPI's)?	5	0	0	5	0	0
Does it exist an arrangement for evaluating in what extent the security policy is used and succeeded?	5	0	3	2	0	0
Focused on economic results:		Very high	High	Less	Very low	Can't answ.
		4	**4**	**2**	**0**	**0**
Is the organization that you are working in focused on economical objectives and results?	5	2	2	1	0	0
In our organization many of the employees are evalutated against economical results.	5	2	2	1	0	0
Learning/awareness:		Very high	High	Less	Very low	Can't answ.
		2	**8**	**4**	**0**	**1**
Is the security policy communicated/teached the employees regurlarly (minimum one time a year)?	5	0	1	4	0	0
The employees in our organization are informed about understanding the importance of security issues related to their work.	5	1	4	0	0	0
Are employees working with ICT infrastructure trained in handling unforeseen security breaches?	5	1	3	0	0	1
SP based on standards/"best practices":		Very high	High	Less	Very low	Can't answ.
		2	**3**	**0**	**0**	**0**
Is preparation of the security policy based on standards or "best practices" (e.g. ISF or equivalents)?	5	2	3	0	0	0
Personal bonding:		Very high	High	Less	Very low	Can't answ.
		2	**2**	**1**	**0**	**0**
We have an arrangement with objective to exchange personal security knowledge between divisions/departments.	5	2	2	1	0	0
SP performs weaker effect than expected:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**4**	**1**	**0**
Has the security policy weaker effect than expected in your organization?	5	0	0	4	1	0

9.6 Appendices F: Low level of resistance.

Low level of resistance (4 respondents)						
Level of resistance:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**5**	**15**	**0**
We have arrangement for preparedness, crisis- and contingency management, which is tested yearly.	4	0	0	1	3	0
We are working a lot in purpose to determine adequate security measures in our organization.	4	0	0	1	3	0
The objectives/directives stated in the Security Policy is highly integrated in the organizations working processes.	4	0	0	2	2	0
Is the organization certified in accordance with an security standard? [*]	4	0	0	0	4	0
Our organization has defined a "security baseline" for system-technical security measures.	4	0	0	1	3	0
Level of loss:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**1**	**7**	**0**
Has your organization realised an essential economical loss due to security breaches caused by own employees (insiders) last year?	4	0	0	0	4	0
Has your organization realised an essential economical loss due to security breaches caused by external unauthorized threats last year?	4	0	0	1	3	0
Poor design of Security Policy:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**1**	**3**	**0**
Have conditions due to poor design of the security policy been direct cause to security breaches during the last year?	4	0	0	1	3	0
Lack of knowledge:		Very high	High	Less	Very low	Can't answ.
		0	**1**	**1**	**2**	**0**
Have conditions due to lack of knowledge of the security policy been direct cause to security breaches during the last year?	4	0	1	1	2	0
Lack of respect:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**2**	**1**	**1**
In what extent are security breaches traceable due to employees lack of respect for the security policy?	4	0	0	2	1	1
Engagement from management:		Very high	High	Less	Very low	Can't answ.
		1	**3**	**5**	**11**	**0**
Our management shows clear and explisit in action that security is important for the organization.	4	0	1	1	2	0
Have you during the last year discussed with your colleagues how to improve your security policy?	4	0	1	3	0	0
Our employees is the most important resources in the aim of acheiving adequate security.	4	1	1	1	1	0
The security policy directs that arrangement for teaching security shall be in place.	4	0	0	0	4	0
Do the budget assign resources for security education?	4	0	0	0	4	0

Focus on behaviour and attitude:		Very high	High	Less	Very low	Can't answ.
		0	**1**	**5**	**10**	**0**
Our organization is clever in communicating behaviour and attitude aspects anticipated from the employees.	4	0	1	1	2	0
We are known with, and communicates the employees regurlarly (monthly) about security threats and risks related to the organizational working tasks.	4	0	0	1	3	0
Is information about security communicated over the intranett?	4	0	0	3	1	0
Is security conversation with the employees accomplished at least one time during the year?	4	0	0	0	4	0
Monitoring/report/follow up:		Very high	High	Less	Very low	Can't answ.
		0	**3**	**1**	**8**	**0**
Has the organization adequate routines for measuring, reporting and following up of faults/incidents in the ICT systems?	4	0	3	1	0	0
Are the employees evaluated regarding performance related to the security policy (balanced scorecard, KPI's)?	4	0	0	0	4	0
Does it exist an arrangement for evaluating in what extent the security policy is used and succeeded?	4	0	0	0	4	0
Focused on economic results:		Very high	High	Less	Very low	Can't answ.
		3	**2**	**1**	**2**	**0**
Is the organization that you are working in focused on economical objectives and results?	4	2	1	0	1	0
In our organization many of the employees are evalutated against economical results.	4	1	1	1	1	0
Learning/awareness:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**1**	**11**	**0**
Is the security policy communicated/teached the employees regurlarly (minimum one time a year)?	4	0	0	0	4	0
The employees in our organization are informed about understanding the importance of security issues related to their work.	4	0	0	0	4	0
Are employees working with ICT infrastructure trained in handling unforeseen security breaches?	4	0	0	1	3	0
SP based on standards/"best practices":		Very high	High	Less	Very low	Can't answ.
		0	**1**	**3**	**0**	**0**
Is preparation of the security policy based on standards or "best practices" (e.g. ISF or equivalents)?	4	0	1	3	0	0
Personal bonding:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**0**	**4**	**0**
We have an arrangement with objective to exchange personal security knowledge between divisions/departments.	4	0	0	0	4	0
SP performs weaker effect than expected:		Very high	High	Less	Very low	Can't answ.
		1	**0**	**2**	**0**	**1**
Has the security policy weaker effect than expected in your organization?	4	1	0	2	0	1

9.7 Appendices G: Security policy weaker than expected

Security Policy (SP) weaker than expected (8 resondents)						
Level of resistance:		Very high	High	Less	Very low	Can't answ.
		4	**16**	**8**	**12**	**0**
We have arrangement for preparedness, crisis- and contingency management, which is tested yearly.	8	1	4	2	1	0
We are working a lot in purpose to determine adequate security measures in our organization.	8	2	4	1	1	0
The objectives/directives stated in the Security Policy is highly integrated in the organizations working processes.	8	0	5	2	1	0
Is the organization certified in accordance with an security standard? [*]	8	0	0	0	8	0
Our organization has defined a "security baseline" for system-technical security measures.	8	1	3	3	1	0
Level of loss:		Very high	High	Less	Very low	Can't answ.
		0	**1**	**3**	**12**	**0**
Has your organization realised an essential economical loss due to security breaches caused by own employees (insiders) last year?	8	0	0	1	7	0
Has your organization realised an essential economical loss due to security breaches caused by external unauthorized threats last year?	8	0	1	2	5	0
Poor design of Security Policy:		Very high	High	Less	Very low	Can't answ.
		0	**1**	**1**	**6**	**0**
Have conditions due to poor design of the security policy been direct cause to security breaches during the last year?	8	0	1	1	6	0
Lack of knowledge:		Very high	High	Less	Very low	Can't answ.
		0	**4**	**3**	**1**	**0**
Have conditions due to lack of knowledge of the security policy been direct cause to security breaches during the last year?	8	0	4	3	1	0
Lack of respect:		Very high	High	Less	Very low	Can't answ.
		1	**2**	**4**	**1**	**0**
In what extent are security breaches traceable due to employees lack of respect for the security policy?	8	1	2	4	1	0
Engagement from management:		Very high	High	Less	Very low	Can't answ.
		12	**11**	**7**	**10**	**0**
Our management shows clear and explisit in action that security is important for the organization.	8	1	4	1	2	0
Have you during the last year discussed with your colleagues how to improve your security policy?	8	5	3	0	0	0
Our employees is the most important resources in the aim of acheiving adequate security.	8	5	2	0	1	0
The security policy directs that arrangement for teaching security shall be in place.	8	1	2	1	4	0
Do the budget assign resources for security education?	8	0	0	5	3	0

Focus on behaviour and attitude:		Very high	High	Less	Very low	Can't answ.
		2	**9**	**12**	**9**	**0**
Our organization is clever in communicating behaviour and attitude aspects anticipated from the employees.	8	0	4	2	2	0
We are known with, and communicates the employees regurlary (monthly) about security threats and risks related to the organizational working tasks.	8	0	2	6	0	0
Is information about security communicated over the intranett?	8	2	3	3	0	0
Is security conversation with the employees accomplished at least one time during the year?	8	0	0	1	7	0
Monitoring/report/follow up:		Very high	High	Less	Very low	Can't answ.
		1	**6**	**6**	**11**	**0**
Has the organization adequate routines for measuring, reporting and following up of faults/incidents in the ICT systems?	8	0	6	2	0	0
Are the employees evaluated regarding performance related to the security policy (balanced scorecard, KPI's)?	8	0	0	1	7	0
Does it exist an arrangement for evaluating in what extent the security policy is used and succeeded?	8	1	0	3	4	0
Focused on economic results:		Very high	High	Less	Very low	Can't answ.
		7	**5**	**2**	**2**	**0**
Is the organization that you are working in focused on economical objectives and results?	8	4	3	1	0	0
In our organization many of the employees are evalutated against economical results.	8	3	2	1	2	0
Learning/awareness:		Very high	High	Less	Very low	Can't answ.
		2	**2**	**13**	**7**	**0**
Is the security policy communicated/teached the employees regurlarly (minimum one time a year)?	8	0	0	3	5	0
The employees in our organization are informed about understanding the importance of security issues related to their work.	8	0	1	6	1	0
Are employees working with ICT infrastructure trained in handling unforeseen security breaches?	8	2	1	4	1	0
SP based on standards/"best practices":		Very high	High	Less	Very low	Can't answ.
		3	**4**	**1**	**0**	**0**
Is preparation of the security policy based on standards or "best practices" (e.g. ISF or equivalents)?	8	3	4	1	0	0
Personal bonding:		Very high	High	Less	Very low	Can't answ.
		0	**4**	**2**	**2**	**0**
We have an arrangement with objective to exchange personal security knowledge between divisions/departments.	8	0	4	2	2	0
SP performs weaker effect than expected:		Very high	High	Less	Very low	Can't answ.
		2	**6**	**0**	**0**	**0**
Has the security policy weaker effect than expected in your organization?	8	2	6	0	0	0

9.8 Appendices H: Security policy not weaker than expected

Security Policy (SP) not weaker than expected (14 respondents)						
Level of resistance:		Very high	High	Less	Very low	Can't answ.
		11	**29**	**11**	**16**	**3**
We have arrangement for preparedness, crisis- and contingency management, which is tested yearly.	14	3	6	3	2	0
We are working a lot in purpose to determine adequate security measures in our organization.	14	2	9	2	1	0
The objectives/directives stated in the Security Policy is highly integrated in the organizations working processes.	14	2	8	2	2	0
Is the organization certified in accordance with an security standard? [*]	14	3	0	0	10	1
Our organization has defined a "security baseline" for system-technical security measures.	14	1	6	4	1	2
Level of loss:		Very high	High	Less	Very low	Can't answ.
		0	**1**	**2**	**24**	**1**
Has your organization realised an essential economical loss due to security breaches caused by own employees (insiders) last year?	14	0	1	1	11	1
Has your organization realised an essential economical loss due to security breaches caused by external unauthorized threats last year?	14	0	0	1	13	0
Poor design of Security Policy:		Very high	High	Less	Very low	Can't answ.
		0	**1**	**5**	**8**	**0**
Have conditions due to poor design of the security policy been direct cause to security breaches during the last year?	14	0	1	5	8	0
Lack of knowledge:		Very high	High	Less	Very low	Can't answ.
		0	**2**	**10**	**2**	**0**
Have conditions due to lack of knowledge of the security policy been direct cause to security breaches during the last year?	14	0	2	10	2	0
Lack of respect:		Very high	High	Less	Very low	Can't answ.
		0	**4**	**5**	**4**	**1**
In what extent are security breaches traceable due to employees lack of respect for the security policy?	14	0	4	5	4	1
Engagement from management:		Very high	High	Less	Very low	Can't answ.
		26	**28**	**10**	**6**	**0**
Our management shows clear and explisit in action that security is important for the organization.	14	3	9	2	0	0
Have you during the last year discussed with your colleagues how to improve your security policy?	14	7	5	2	0	0
Our employees is the most important resources in the aim of acheiving adequate security.	14	11	3	0	0	0
The security policy directs that arrangement for teaching security shall be in place.	14	4	6	1	3	0
Do the budget assign resources for security education?	14	1	5	5	3	0

Focus on behaviour and attitude:		Very high	High	Less	Very low	Can't answ.
		9	**17**	**19**	**11**	**0**
Our organization is clever in communicating behaviour and attitude aspects anticipated from the employees.	14	2	9	2	1	0
We are known with, and communicates the employees regurlarly (monthly) about security threats and risks related to the organizational working tasks.	14	1	2	6	5	0
Is information about security communicated over the intranett?	14	5	5	4	0	0
Is security conversation with the employees accomplished at least one time during the year?	14	1	1	7	5	0
Monitoring/report/follow up:		Very high	High	Less	Very low	Can't answ.
		0	**20**	**11**	**11**	**0**
Has the organization adequate routines for measuring, reporting and following up of faults/incidents in the ICT systems?	14	0	14	0	0	0
Are the employees evaluated regarding performance related to the security policy (balanced scorecard, KPI's)?	14	0	0	7	7	0
Does it exist an arrangement for evaluating in what extent the security policy is used and succeeded?	14	0	6	4	4	0
Focused on economic results:		Very high	High	Less	Very low	Can't answ.
		9	**8**	**6**	**5**	**0**
Is the organization that you are working in focused on economical objectives and results?	14	5	4	4	1	0
In our organization many of the employees are evalutated against economical results.	14	4	4	2	4	0
Learning/awareness:		Very high	High	Less	Very low	Can't answ.
		6	**16**	**12**	**7**	**1**
Is the security policy communicated/teached the employees regurlarly (minimum one time a year)?	14	1	4	6	3	0
The employees in our organization are informed about understanding the importance of security issues related to their work.	14	4	7	1	2	0
Are employees working with ICT infrastructure trained in handling unforeseen security breaches?	14	1	5	5	2	1
SP based on standards/"best practices":		Very high	High	Less	Very low	Can't answ.
		6	**6**	**1**	**1**	**0**
Is preparation of the security policy based on standards or "best practices" (e.g. ISF or equivalents)?	14	6	6	1	1	0
Personal bonding:		Very high	High	Less	Very low	Can't answ.
		2	**2**	**5**	**4**	**1**
We have an arrangement with objective to exchange personal security knowledge between divisions/departments.	14	2	2	5	4	1
SP performs weaker effect than expected:		Very high	High	Less	Very low	Can't answ.
		0	**0**	**8**	**6**	**0**
Has the security policy weaker effect than expected in your organization?	14	0	0	8	6	0

9.9 Appendices I: Monitoring security policy

Monitoring security policy (7 respondents)						
SP highly integrated in working processes:		Very high	High	Less	Very less	Can't answ.
		0	**7**	**0**	**0**	**0**
The objectives/directives stated in the Security Policy is highly integrated in the organizations working processes.	7	0	7	0	0	0
Arrangement for following up SP in place:		Very high	High	Less	Very less	Can't answ.
		1	**6**	**0**	**0**	**0**
Does it exist an arrangement for evaluating in to what extent the security policy is used and succeed?	7	1	6	0	0	0
Conformity between policy and practice:		Very high	High	Less	Very less	Can't answ.
		0	**6**	**1**	**0**	**0**
Do you experience conformity between what is written in the security policy and practical experience in your organization.	7	0	6	1	0	0
SP performs weaker effect than expected:		Very high	High	Less	Very less	Can't answ.
		0	**1**	**2**	**4**	**0**
Has the security policy weaker effect than expected in your organization?	7	0	1	2	4	0