NTNU – Trondheim
Norwegian University of
Science and Technology

Information Security Metrics An Empirical Study of Current Practice

Marte Tårnes

Specialization Project

Trondheim, 17th December 2012

Supervisor: Maria B. Line, NTNU/SINTEF
Responsible professor: Svein Johan Knapskog, NTNU

Norwegian University of Science and Technology
Department of Telematics

Abstract

Information security is a growing concern in many organizations and measuring information security is difficult. Information security metrics can be used to monitor how well you have reached you security goals and to increase the understanding of information security. A metric is defined as being a system or standard for measurement. There exist metrics proposed by various organizations, as well as by researchers, but there is limited research on the use of metrics in practice.

This project includes an empirical study, based on in-depth interviews of various organizations. The goal of this study is to examine to what extent information security metrics are used, how they are used and how organizations benefit from it.

The results showed that few measurements related to information security were performed and that there was a general lack of systems for measurement. This indicates that the area of information security metrics is immature in the participating organizations.

Preface

This study is submitted to the Norwegian University of Science and Technology (NTNU) as a part of the five-year program Master of Science in Communication Technology at the Department of Telematics (ITEM).

I would like to thank my supervisor Maria B. Line and My professor Svein Johan Knapskog for valuable comments and guidance throughout this study. I would also like to thank the interviewees that took the time to participate in the empirical study

Trondheim, 17th December 2012

Marte Tårnes

Contents

List of Figures

List of Tables

Acronyms

ACSA Applied Computer Security Associates

ALE Annualized Loss Expectancy

ARO Annualized Rate of Occurrence

CIS Center for Internet Security

ERP Enterprise Resource Planning

IDS Intrusion Detection System

IEC International Electrotechnical Commission

IS Information Security

ISMS Information Security Management System

ISO International Organization for Standardization

NIST National Institute of Standards and Technology

NorCERT Norwegian Computer Emergency Response Team

NSM Nasjonal Sikkerhetsmyndighet

PDCA Plan-Do-Check-Act

ROI Return On Investment

SDLC System Development Life Cycle

SLE Single Loss Expectancy

TCO Total Cost of Ownership

Chapter 1

Introduction

Information security is a growing concern in many organizations and in many cases crucial to their operations. But how can an organization know if their implemented information security controls and management are sufficient? This report concerns information security metrics, in theory and in practice.

1.1 Problem Definition

This study focuses on how information security metrics are used in practice. In particular it contains a background study of existing metrics, an empirical study based on interviews and a discussion and comparison of theoretical procedures and observed practices. The main goal of the empirical study is to examine if metrics are used in practice in various companies and organizations[1], how the metrics are used and how the organizations benefit from it. A partial goal of this study is to examine if current practice corresponds with existing suggested practice from literature. This is accomplished by performing interviews of various organizations.

[1]Throughout the report the word organization will be used to cover any type of company or organization.

1.2 Motivation

The main motivations for this project are that there is limited empirical research related to this subject and it is both an interesting and difficult area. There exist many books, research papers, and several standards related to information security metrics, but there are few studies that examine the use of metrics in practice.

1.3 Limitations

The empirical study includes only a small number of organizations and therefore a generalization will not be possible. Any comparisons of the organizations will therefore not be performed, rather between each organization and theory from existing standards, books and research papers. Challenges and limitations related to the method used for the empirical study are discussed in section 3.3.

1.4 Outline

Chapter 2 presents a background on information security metrics. This includes what information security is in addition to proposed metrics, standards and a guideline. The method used for the empirical study is presented in chapter 3. The results of the empirical study is presented in chapter 4. Chapter 5 discusses the results presented in chapter 4 and compares these with theory presented in chapter 2. Chapter 6 includes a conclusion of the findings and suggestions for future work. Appendix A contains an information sheet, given to the participating organizations. Appendix B contains the interview guide used as a basis for the collection of empirical data for this study. Both of the appendices are written in Norwegian.

Chapter 2

Background

This chapter gives an introduction to information security metrics including specific existing metrics, a standard and a set of guidelines.

2.1 Information security metrics overview

Information security metrics are about measuring information security, but it can be a bit difficult to understand exactly what it is, especially as various books and papers seem to have somewhat different definitions. The Oxford Dictionaries define the word metric as a system or standard of measurement. Several papers and articles like [1] and [2] say that metrics should be SMART, i.e. specific, measurable, attainable, repeatable/relevant and time-dependent/timely. Even though the definitions are somewhat different the essence is the same. A workshop organized by the Applied Computer Security Associates (ACSA) and the MITRE Corporation [3] defines it in the following way:

> "An Information Security (IS) metric[1] is a value, selected from a partially ordered set by some assessment process, that represents an IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence."

[1] This workshop used the term (IS)* where the asterisk could mean metric, measure, score, rating, rank or assessment result, however metric was the word that tended to be used the most.

National Institute of Standards and Technology (NIST) [4] defines it like this:

> "Information security measures[2] are used to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements."

Even though this last definition does not use the word metric they are still talking about the same thing and information security metrics seem to be about collection, analysis, prediction and improvement and they should be specific. The rest of this section is going to take a closer look at information security metrics.

2.1.1 Metrics vs measurements

In various books and papers you can find the words metric, measure and measurement used somewhat interchangeably. NIST for example uses metrics in one version of a document and then changes to measure in the first revision. There does however seem to be a common understanding that measurements is about making observations [5] and that these are at a single point in time [1]. Metrics on the other hand are about analysis and comparison [1]. They are supposed to give you information about IT Security [5]. Andrew Jaquith defines metric as being a standard of measurement [6]. The standard ISO/IEC 27004 defines measurement as the process of obtaining information about the effectiveness of Information Security Management System (ISMS) controls [7]. The same standard defines measure as being a variable to which the result of a measurement is assigned. The term indicator is also something that comes up in the literature in relation to metrics, measures and measurements. ISO/IEC 27004 defines an indicator in the following way:

[2] It is important to note that the word measures in this case does not mean actions, but metrics. The first version from 2003 uses the word metrics here, but revision 1 from 2008 uses the word measures. The definitions in the two versions are not word-by-word identical, but essentially they say the same. Measures in the context of this document mean the results of data collection, analysis, and reporting.

> "Measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs"

In [8] the term indicator is used for observable measures that provide insights into a concept that is difficult to measure directly. It defines a metric as being the system of measurement used to collect and report that indicator. An indicator and its interpretation constitute the measurement result [7].

2.1.2 Why use metrics

Lance Hayden states in [5] that one measures security to understand it and W. Krag Brotby states in [9] that "you can't manage what you can't measure". The latter statement is presented in several papers and reports as an accepted principle. This points to two of the most important aspects of information security metrics, understanding and management. This is supported in [6], where the goal of metrics is stated as being to quantify data to facilitate insight. While the security threat level increases, the level of understanding security actually seems to be worsened and important actions are not taken [10]. The study that reports these results, which was conducted in Norway, claims that organizations and companies do not have knowledge about neither threats nor actual incidents and that there are probably a lot of incidents not reported and not even discovered. There appears to be a need for better security understanding and awareness. The use of metrics could contribute to achieve this.

Fully understanding security is important both in development and management. Reijo Savola believes that in order to get a holistic understanding of security we should use common approaches to metrics in different security disciplines [11]. It is also stated that metrics can help you characterize, evaluate, predict and improve. Metrics can monitor how well you have reached your security goals and objectives. They can also be used to justify and direct future security investments [12].

Metrics can help identify the level of risk in not taking an action, and in that way it could help decision makers in prioritizing actions. In addition to increase understanding, the use of metrics could also contribute to raising the security awareness in an organisation. [1] As we can see, there are several reasons why metrics can be useful in an organization. Many people may think about security as only being about incidents, but it is important to

remember that it is about much more. William Stallings in [13] defines it in the following way:

> "The field of **network and Internet security** consists of measures[3] to deter, prevent, detect, and correct security violations that involve the transmission of information."

It might be the case that the number of incidents is observed and the results of these observations are used to evaluate the security of the organization. The situation may then be that it looks like the organization is very good at preventing incidents. This may be the truth, but the situation may also be completely different and the reason why there have not been many incidents could be that there have not been many attempts of intrusion. How can one know the difference between having good systems for information security and just being lucky, if the number of incidents is the only measurement in use? It gives no indications related to other factors of security, such as correcting security violations. As security seems to involve many aspects, it is a natural conclusion to draw that security metrics should do the same, and if they do, they could be a help in evaluating an organization's security.

2.1.3 How to use metrics

What type of metric to choose and how to use them depend on the type of organization in question as well as the types of programs, systems, processes etc. that are in use and that one wants to evaluate. As an organization and its use of security programs mature, the use of metrics will change. It is important to choose a metric that utilizes data that can actually be obtained from existing processes in the organization [12]. In any case there seems to be a common understanding that metrics is about analysis and understanding of the results and not about collecting as much data as possible. The whole point is that you are supposed to be able to use it for something.

Andrew Jaquith writes that one has to measure both the threat and the incident and controls [6]. This will contribute to finding out why some incidents happen and some do not. Secondly he emphasizes that one needs models that can provide rationales for measurement. These models can be copied from other industries that have more experience when it comes to measurement. This could be industries like insurance, public health,

[3]Note that in this case measures means actions and is not related to the word metrics.

quality assurance and finance. He states that a good metric should have the following properties:

- Consistently measured, without subjective criteria
- Cheap to gather, preferably in an automated way
- Expressed as a cardinal number or percentage, not with qualitative labels like "high", "medium", and "low"
- Expressed using at least one unit of measure, such as "defects", "hours", or "dollars"
- Contextually specific, relevant enough to decision-makers so that they can take action

In [10] we see that there is a substantial gap between estimated and reported incidents. As mentioned, this may partly be because many incidents are not even discovered. Some organizations are more exposed to attacks than others, and some may experience fewer incidents than others due to pure luck. There are many factors related to why some organizations may experience more attacks than others. Therefore observing the number of incidents may not be a good way of measuring the security of an organization, as mentioned in [1].

An organization can choose to use an existing security metrics program or they can build their own. If the latter strategy is chosen, SANS Institute advices in [1] to use the following guidelines:

1. Define the metrics program goal(s) and objectives
2. Decide which metrics to generate
3. Develop strategies for generating the metrics
4. Establish benchmarks and targets
5. Determine how the metrics will be reported
6. Create an action plan and act on it, and
7. Establish a formal program review/refinement cycle

It is important to clearly state the goal and objectives of the program, and having one single goal is stated to be a good approach. This is the first step. In step 2 the metrics to generate should both be chosen and well understood. When this is done the strategies for actually generating these metrics should be specified in detail including where to get the data from and how often the data will be collected, in step 3. Step 4 includes comparison with the industry or with a best practice if there is one. This could help an organization to establish targets. There is no point in using security metrics

if the results of the measurements are not really used. Additionally, all measurement results should not necessarily be presented to the same people. To make the most of the use of security metrics it is important to determine in advance how the results should be reported and this is done in step 5. Items in the action plan, created in step 6, should be directly derivable from the objectives specified in step 1. The program should continuously be reviewed and if needed refined. This includes asking critical questions related to the program as well as research related to standards and best practices. [1]

The type and number of security metrics program(s) to be used in an organization, as well as how to use them, depend on the size and complexity of the organization. A small organization will for example in many cases manage with a small simple program whereas a large complex company may need several and complex programs. [7]

Section 2.3 describes a standard and a guideline for measurement that can be used as a basis for the development of a measurement process.

2.1.4 Qualitative vs. quantitative metrics

Qualification is subjective and reflects human opinions and human judgment. Quantification is objective and is based on real numbers. [5, 7]

2.1.5 Security metrics analysis

Using metrics is all about being able to use them to improve your understanding or knowledge about something. A program is only a security metrics program if the data collected is actually used for something. Additionally, someone needs to understand every metric as well as why that specific metric is used and why, meaning what the metric is supposed to help you with [5].

2.1.6 Presenting the metrics to the organization

Metrics must, as discussed, be analysed to be of value, but to whom should the measurement results be presented and how? Usually such issues should be presented to decision makers as they are the ones deciding if actions are

to be taken and investments are to be made. The challenge is to present security metrics to someone who does not know much about it. Andrew Jaquith claims that presentations for CEOs tend to be dumbed down and that simplicity is often mistaken for clarity [6, 14].

2.2 Existing and proposed metrics

There exist a number of security metrics and this section discusses a selection of them. Some of these metrics are derived from finance, where metrics are much more prevalent than they are in information security, and some of them are simpler and more intuitive. Annualized Loss Expectancy (ALE), Return On Investment (ROI) and Total Cost of Ownership (TCO) are metrics derived from finance whereas Baseline Defence Coverage, Patch Latency, Password Strength and Platform Compliance Scores are easier to both use and understand. One important aspect to remember is that only one metric will usually not give a holistic picture of the state of the security in the organization, as we will see throughout this section. The last five metrics are proposed in NIST SP 800-55 [4], and are quantitative and quite specific. Note that NIST SP 800-55 uses the word measure as defined in section 2.1.

2.2.1 Risk Assessment Matrix

Risk is something that it is useful to have knowledge of, but that is hard to measure partly due to the existence of many different definitions. The risk assessment matrix is one proposal for measuring risk. This matrix could exist in several forms, but one simple generic version is showed in Figure 2.1. This matrix depicts the likelihood and the severity of impact of an event. If the severity of impact is high and the likelihood is also high we can see that we have a problem. This is all good and well except from the fact that it is quite difficult to know or find the likelihood and severity of events. This matrix will in any case be subjective and taking this as an actual measurement of risk would be wrong. What this actually measures is human judgement about risk. That could of course be useful, but it is important that one does not use this metric thinking that risk is what is being measured. [5]

		Likelihood of Event		
		High	Medium	Low
Severity of Impact	High	"We're Doomed!"	Bad	Outlier
	Medium	Bad	Not Good	Error
	Low	Annoyance	Typical	"Whatever..."

Figure 2.1: A generic risk assessment matrix [5]

2.2.2 Annualized Loss Expectancy (ALE)

This is a commonly used conceptual metric that is about how much you think you will lose as a result of a specific security incident. It is pitched as a qualitative metric and is described by the following formula:

$$ALE = ARO * SLE$$

where ARO is the Annualized Rate of Occurrence and SLE is the Single Loss Expectancy. ARO is an indication of how often you expect to experience a specific loss in a given year. SLE is an indication of how much you expect one incident of this loss to cost. The result could help figure out if a security investment is worth the cost, however this metric is quite subjective as it involves people's expectations. It measures what people think, and not actual reality. If it is used without taking that into consideration it may contribute to bad decision making. [5]

Some, like Andrew Jaquith, thinks that this metric is useless because the loss expectancy is a wild guess [6, 14]. It could be easy to measure the cost of a server being inoperable for a day, but what about intangible things like brand reputation? It will be difficult to get this right [5]. Others, on the other hand, admit the disadvantages of the method, but still find it useful. One thing that can help the estimation is to look at historical data for your organization, regarding incidents, brand damage and fines. It is also reasonable to believe that one gets better at this with more experience. As with most other metrics, it could be useful if used in the right setting where it is reasonably easy to estimate the loss. In addition, it could be used as an argument to justify certain security measures. [15]

2.2.3 Return On Investment (ROI)

This metric is about how much benefit you will gain from an investment. It is a metric directly taken from the business world. ROI is related to ALE in the sense that ROI is defined by the relationship between the expected loss in an incident (ALE) and the cost of taking a preventive action. It is used, among other places, in marketing to show that a product is worth the investment. This is a meaningful metric in the business world, but when it comes to security, investments are not made directly to make money, as they often are in other cases. As ROI uses ALE it also has the same issues, namely that parts of the data used are only estimates. When used in marketing more issues arise, as there exists an incentive to actually manipulate data. [5]

The use of ROI may cause companies to choose the wrong technology because they want to save money and they base their decisions too much on ROI and not enough on other aspects to the security investment. The usage of ROI seems to be dropping, possibly due to the difficulties mentioned. [15]

2.2.4 Total Cost of Ownership (TCO)

This metric tries to quantify the total sum of money spent on a system. This includes the purchase price as well as any other costs related to the system throughout the lifetime of the system. TCO could be good for quantifying costs and for comparisons of systems. Another advantage is that it might not as easily become a qualitative metric as the metrics discussed above,

however just like the other metrics discussed it does not really tell you anything about how good the security system is [5]. It is also worth noting that some costs may not easily be foreseen and a complete picture, i.e. a completely correct TCO, will be difficult to derive. TCO could also be used for systems already in use to make decisions about whether they should be replaced or not. [15]

2.2.5 Baseline Defences Coverage

This is a group of metrics that gives information about how well an organization's network is protected against the most basic information security threats. The measurement is carried out by scanning the network to find devices and subsequently check how many of these devices are covered by basic security tools like antivirus, antispyware, Intrusion Detection Systems (IDSs) and firewalls. The result can be presented as a percentage. This is a simple and informative metric as long as it is not assumed to be more than it claims to be. This metric could be improved or made more advanced by dividing the organization into units based on for example departments. This could help uncover tendencies and see where actions should be taken. Another factor that can be taken into account is time related to the security tools, like the age of the virus definitions. If the organization has a 98% coverage when it comes to antivirus, but the virus definitions are really old, the metric could be useless or even misleading. [6, 14]

2.2.6 Patch Latency

This metric gives information about how well an organization's network is up to date when it comes to patches. Patch latency is the time-lag between the release of a patch and the organization's deployment of that patch. As with the previous metric, the measurement is carried out by scanning computers on the network to find out which patches are missing from each machine. One could analyse this metric with respect to various units of the organization as well. In addition, it could be useful to compare average latency in patches with average latency in exploits. If an exploit of a vulnerability is released before stations on the organization's network have been patched, it indicates that the organization's network is not as secure as it could have been. In addition to latency one could use other

metrics related to patch management, such as the percentage of hosts not compliant to policy patch level. [6, 14]

2.2.7 Password Strength

This is a way of finding and eliminating the use of weak passwords in a network. Typically the focus will initially be on the most important systems. There are several available password cracking programs one can use. When using this metric it would be advisable to be a bit careful, as the goal is to improve security and not to punish any users by public announcements. The result can be expressed as the average time it takes to crack passwords. This method could be used to raise security awareness by demonstrating or presenting results to users. This might make them see the real importance of strong passwords [6, 14]. The use of this metric may not be compliant with laws and regulations related to privacy in all countries.

2.2.8 Platform Compliance Scores

This metric involves using existing tools, like tools from the Center for Internet Security (CIS), that run tests against an organization's system to examine if the configuration and hardening of their hardware meet best practice standards. These tools test whether ports are left unnecessarily open, machines are indiscriminately shared and default permissions are left on. [6, 14]

2.2.9 Vulnerability Management

The goal of this measure/metric is to ensure that all vulnerabilities are identified and mitigated. The result is calculated by dividing the number of high[4] vulnerabilities identified and mitigated within a targeted time frame during the time period by the number of high vulnerabilities identified within the time period. The target percentage should be a high percentage defined by the organization using the measure. This is defined as being an effectiveness/efficiency measure and the result gives an indication of the timeliness of a security control implementation. The organization needs to specify a frequency for collection and a frequency for reporting. This

[4] On the scale "Low", "Medium", "High"

could e.g. be monthly or quarterly. The data used in this measure can be obtained from vulnerability scanning software, audit logs, vulnerability management systems, patch management systems and change management records. The report format is suggested to be a stacked bar chart that will illustrate results over several reporting periods. [4]

2.2.10 Access Control

The goal of this measure/metric is to restrict access to information, systems and components to individuals or machines that are identifiable, known, credible and authorized. The result can be calculated by dividing the number of remote access points used to gain unauthorized access by the total number of remote access points. The target result for this is a low percentage defined by the organization. This is defined as being an effectiveness/efficiency measure and it gives an indication of the robustness of a security control implementation. The organization should specify a frequency for the collection and a frequency for the reporting. This measure can get its data from incident databases, audit logs, network diagrams and IDS logs and alerts. The proposed report format is a stacked bar chart that shows results for each month. [4]

2.2.11 Contingency Planning

The goal of this measure/metric is to establish, maintain and effectively implement plans for emergency response, backup operations and post-disaster recovery for information systems. These plans are supposed to ensure the availability of critical resources in emergency situations. The result is calculated by dividing the number of information systems that have conducted annual contingency plan testing by the number of information systems in the system inventory. The target percentage is a high percentage defined by the organization. This is defined as being an effectiveness/efficiency measure and gives information about the robustness of a security control implementation. The organization should also have defined collection and reporting frequencies. The data source of this measure is results from contingency plan testing. The suggested report format is a pie chart showing the percentage of systems that have conducted regular contingency plan testing relative to those that have not. [4]

2.2.12 Maintenance

The goal of this measure/metric is to perform periodic and timely maintenance on information systems and provide effective controls on the tools, techniques, mechanisms and personnel used to conduct information systems maintenance. The result is calculated by dividing the number of system components that undergo maintenance in accordance with formal maintenance schedules by the total number of system components. The target result is a high percentage defined by the organization. This is defined as being an effectiveness/efficiency measure and it gives an indication of the timeliness of a security control implementation. The organization should also have defined collection and reporting frequencies. The data sources of this measure are the maintenance schedule and maintenance logs. The suggested report format is a pie chart showing the percentage of systems that have received maintenance in accordance with formal schedules relative to the percentage of systems that have not. [4]

2.2.13 System and Services Acquisition

The goal of this measure/metric is to ensure that third-party providers employ adequate security measures to protect outsourced information, applications and/or services. The result is calculated by dividing the number of system and service acquisition contracts that include security requirements and specifications by the total number of system and service acquisition contracts. The target result is a high percentage defined by the organization. This measure is defined as being an implementation measure and can be used to demonstrate progress in the implementation of information security programs, security controls and associated policies and procedures. The organization should specify target collection and reporting frequencies. The data sources of the measure are service acquisition contracts. The proposed report format is a pie chart showing the percentage of system and service acquisition contracts that include security requirements and/or specifications relative to the percentage of contracts that do not. [4]

2.3 Standards and guidelines for security metrics

There exist standards and guidelines for information security metrics. This section gives an introduction to one standard and one publication containing guidelines for information security metrics.

2.3.1 ISO/IEC 27004

This subsection gives an introduction to the standard ISO/IEC 27004 and the content is, unless specified otherwise, derived from [7]. This standard is part of the ISO/IEC 27000 family of standards. The standard aims to provide guidance on development and use of measures and measurements to be able to assess the effectiveness of an implemented ISMS and controls[5] or group of controls as specified in ISO/IEC 27001 [17]. These measures and measurements will help to determine whether any ISMS processes or controls need to be improved. The standard defines the implementation of this as an Information Security Measurement Programme. The Information Security Measurement Programme performs identification of inefficient processes or controls. Additionally, it provides assistance regarding the prioritization of actions related to the improvement of these identified processes and controls. It could also be used to demonstrate ISO/IEC 27001 compliance. The Information Security Measurement Programme encourages the organization to provide reliable information to relevant stakeholders concerning its information security, risks and the status of their ISMS. The organization should evaluate the effectiveness of the Implemented Information Security Measurement Programme at planned intervals. They should also evaluate the usefulness of developed measurement results. ISO/IEC 27001 requires organizations to measure the effectiveness of implemented security controls and to specify how this is to be done.

The standard states that the size and complexity of the organization will be relevant for determining what kind of measurements that are needed. Other important factors to consider are applicable requirements (e.g. legal), costs and benefits, risk acceptance and the role of information security in support of the organization's overall business activities.

[5] A control is in ISO/IEC 27002 defined in the following way: "means for managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature" [16]

ISO/IEC 27001 describes how an organization can establish, implement, operate, monitor, review, maintain and improve its ISMS. This can be illustrated by the Plan-Do-Check-Act (PDCA) model as shown in Figure 2.2. The figure shows how one can use the PDCA cycle to go from having information security requirements and expectations to having managed information security. [17]

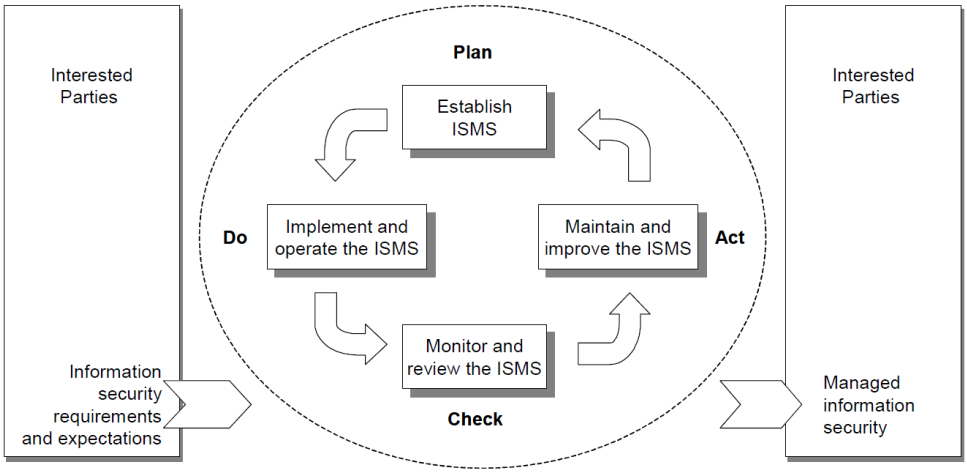

Figure 2.2: The PDCA model applied to ISMS processes [17]

ISO/IEC 27004 defines the following success factors:

a) Management commitment supported by appropriate resources;
b) Existence of ISMS processes and procedures;
c) A repeatable process capable of capturing and reporting meaningful data to provide relevant trends over a period of time;
d) Quantifiable measures based on ISMS objectives;
e) Easily obtainable data that can be used for measurement;
f) Evaluation of effectiveness of Information Security Measurement Programme and implementation of identified improvements;
g) Consistent periodic collection, analysis, and reporting of measurement data in a manner that is meaningful;
h) Use of the measurement results by relevant stakeholders to identify needs for improving the implemented ISMS including its scope, policies, objectives, controls, processes and procedures;
i) Acceptance of feedback on measurement results from relevant stakeholders; and

j) Evaluations of the usefulness of measurement results and implementation of identified improvements.

The standard explains how to relate input and output of measurements to the PDCA cycle. This is illustrated in Figure 2.3. The numbers in the figure represent sub-clauses from ISO/IEC 27001. When developing an Information Security Measurement Programme one should consider the scale and complexity of the ISMS. The standard describes an information security measurement model, which links an information need to the relevant objects of measurement and their attributes. Figure 2.4 illustrates the information security model. A base measure is the simplest measure that can be obtained. It is obtained by applying a measurement method on several attributes of an object of measurement. Objects of measurement can among other things be performance of controls or processes, behaviour of personnel, and activities of units responsible for information security. The measurement method seeks to quantify an attribute through a sequence of operations. Examples of sources of the measurement method could be risk analysis results, audit reports, logs, incident reports, test results and questionnaires. The measurement method may be subjective or objective, where subjective methods rely on qualification and objective methods use quantification. A derived measure is an aggregate of two or more base measures. The measurement function is used to combine the base measures together by performing a calculation. An analytical model is applied to a base and/or a derived measure to obtain an indicator. It combines relevant measures in a way that produces an output that makes sense for the stakeholders. To arrive at a result the indicators must be interpreted. This is done based on some defined decision criteria. The decision criteria are used to determine whether any actions need to be taken and to describe the level of confidence in the measurement results. The results should be considered in the context of the overall measurement objectives. It is important that the measurement method is consistent over time, so that values assigned to base measures, derived measures and indicators are comparable.

The standard states that the management is responsible for establishing the Information Security Measurement Programme and for involving relevant stakeholders in the measurement activities. The involvement of stakeholders includes ensuring that they are trained adequately and understand their duties. The stakeholders should also participate in defining the measurement scope. Examples of stakeholders are the information owner, the information collector, the information communicator and the client for measurement. The

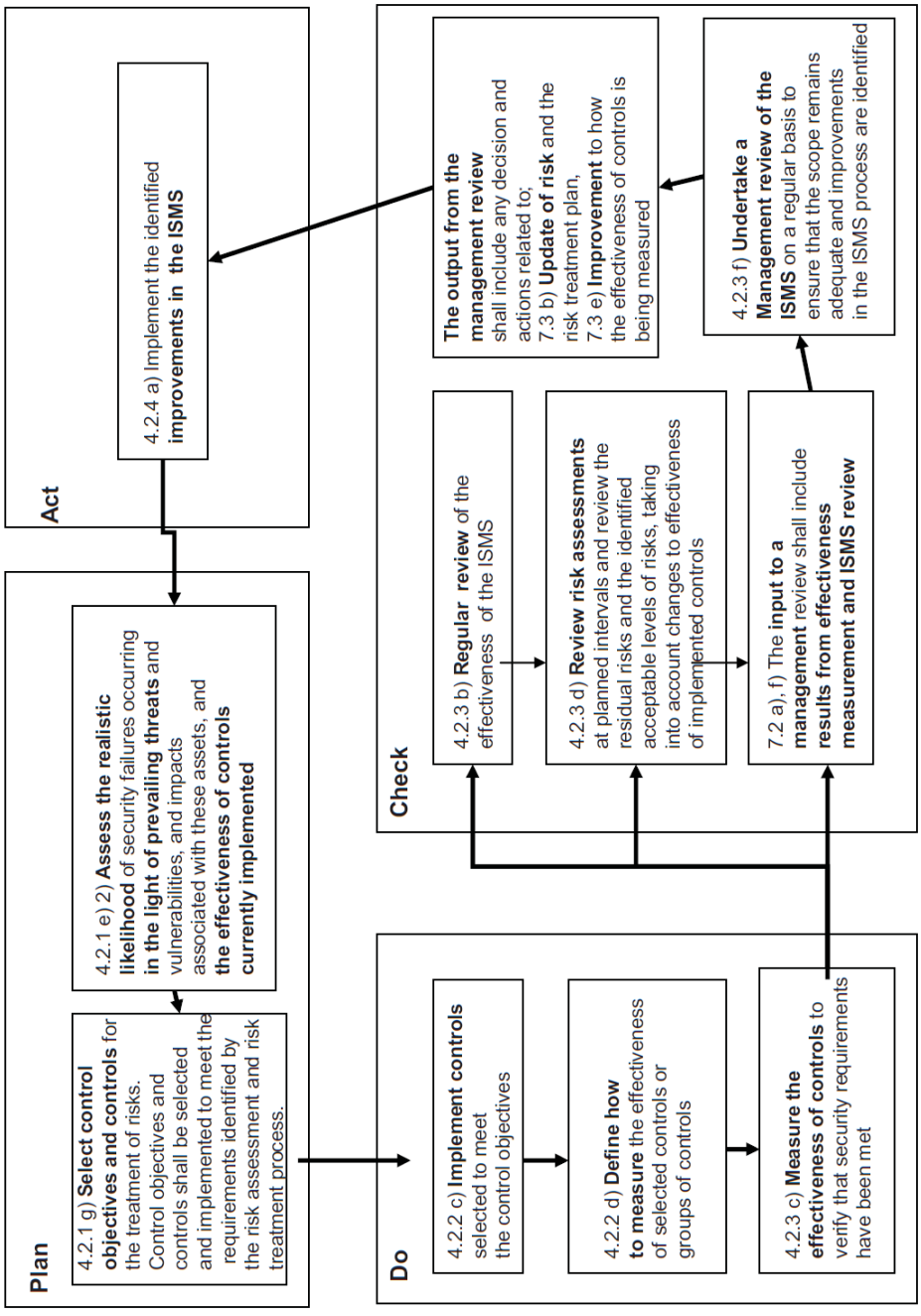

Figure 2.3: Measurement input and output in the ISMS PDCA cycle [7]

client for measurement is the management or another interested party that requests or requires information about the effectiveness of the ISMS, controls or group of controls. The management also needs to use measurement results as input to management reviews and in improvement activities within the ISMS. In addition, the management should assign and provide resources to facilitate measurements.

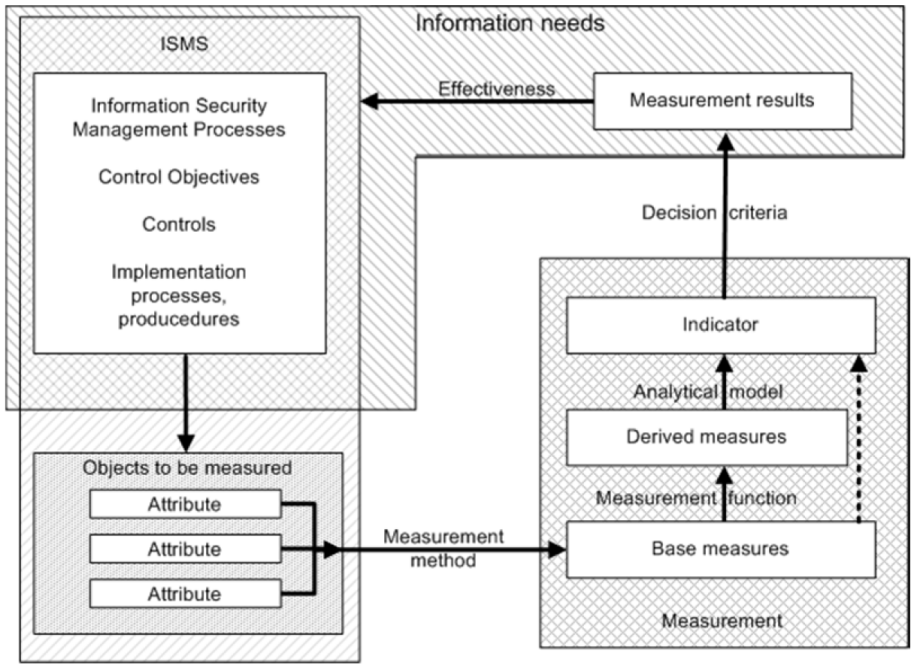

Figure 2.4: Information security measurement model [7]

When an organization for the first time initiates processes related to measurement their activities may be limited, depending on the organization's capabilities and resources. Over time the activities can be widened. It is important that all selected measures are based on information needs. An information need is defined as being insight necessary to manage objectives, goals, risks and problems. The reason for choices regarding measures, objects and attributes should be documented.

The results from measurements must be analysed. This analysis should identify gaps between expected and actual measurement results. Procedures for reporting of results should be stated. Examples of report formats are scorecards providing strategic information, reports, operational dashboards

and gauges representing dynamic values. It is the information communicator that is responsible for determining how to communicate the results.

2.3.2 NIST SP 800-55

This subsection gives an introduction to NIST Special Publication 800-55 and the content is, unless specified otherwise, derived from [4]. NIST SP 800-55 is a guideline that is supposed to assist in the development, selection and implementation of measures to be used at the information system- and program-level. The definition of the term measures that this guideline uses is stated in section 2.1 of this report. These measures will say something about the effectiveness of security controls applied to information systems and supporting information security programs. They can also be used to justify information security investments and support risk-based decisions. NIST SP 800-55 uses controls identified in NIST SP 800-53 [18] as a basis for the development of measures, but the process could also be used for other controls. The guideline defines some factors that must be considered during the development of an information security measurement program:

a) Measures must yield quantifiable information (percentages, averages, and numbers);
b) Data that supports the measures needs to be readily obtainable;
c) Only repeatable information security processes should be considered for measurement; and
d) Measures must be useful for tracking performance and directing resources.

The guideline defines four interdependent components of an information security measurement program. The structure of such a program is illustrated in Figure 2.5. The figure shows a foundation of a strong upper-level management support. This foundation establishes a focus on security within the management. This is critical to avoid failure if the organization is pressured by organizational dynamics and budget limitations.

The second component is practical information security policies and procedures. Policies and procedures are necessary in order to obtain data to be used for measurement. At the same time this component is dependent on being backed by the management. The third component is developing and establishing quantifiable performance measures. These measures must be based on information security performance goals and objectives, easily

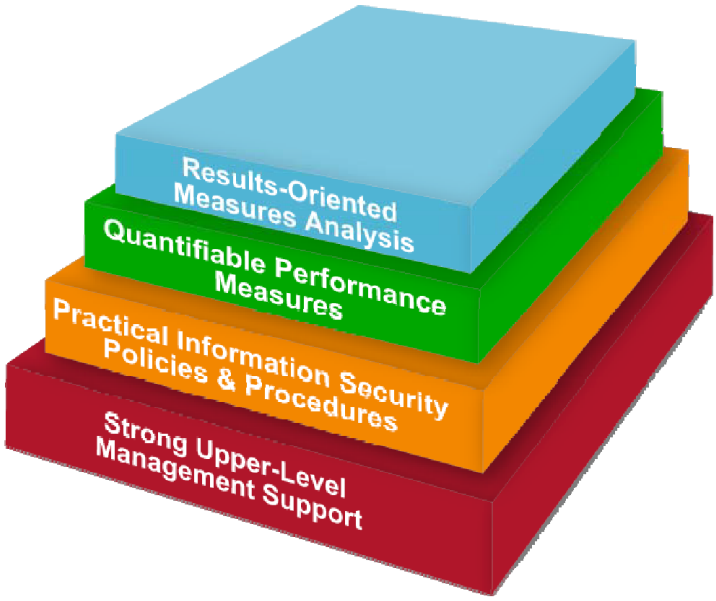

Figure 2.5: Information security measurement program structure [4]

obtainable, feasible to measure, repeatable and provide relevant performance trends over time. The fourth component is a result-oriented measures analysis. This analysis must be periodic and consistent. The results of the analysis can be used to improve the effectiveness of existing security controls, and plan for the implementation of future security controls. The success of an information security program is determined by the degree of meaningful measures it produces.

The information security performance goals and objectives of an organization are supposed to be the basis for their information security measures. The information security measures monitor the accomplishment of these goals and objectives. The monitoring consists of several actions:

- A quantification of the implementation, efficiency and effectiveness of security controls;
- An analysis of the adequacy of information security program activities; and
- An identification of possible improvement actions.

The guideline describes several benefits of using measurements:

Increase Accountability: This happens when measures identify specific security controls that are implemented incorrectly, are not implemented or are ineffective.

Improve Information Security Effectiveness: Measures can contribute to this being accomplished by relating results of information security activities and events to security controls and information security investments.

Demonstrate Compliance: Measures can be used to demonstrate compliance with laws, rules and regulations.

Provide Quantifiable Inputs for Resource Allocation Decisions: Measures related to past or current failures or successes of information security investments can be used to support risk-based decision making.

The maturity of the security control implementation determines what type of measures can realistically be obtained and be useful. The guideline defines implementation measures, effectiveness/efficiency measures and impact measures.

Implementation Measures Implementation measures are used in relation to the progress of the implementation of information security measurement programs, security controls and associated policies and procedures. An example of such a measure is *the percentage of information systems with password policies configured as required.* These measures can also examine system-level areas. An example of that is *the percentage of servers within a system with a standard configuration.* These percentages will likely be less that 100 percent to begin with and as the program matures they will increase. As the percentages reach and remain at 100 percent, as they should, the organization should shift their focus towards effectiveness/efficiency and impact measures. Even though they should shift their focus, they should not retire the implementation measures completely.

Effectiveness/Efficiency Measures Effectiveness/efficiency measures are used to monitor if processes and security controls are implemented correctly, operating as intended and meeting the desired outcome. Effectiveness in this context refers to the robustness of the security control implementation result and efficiency refers to the timeliness of it. An example of a measure that relies on information regarding effectiveness (and implementation) is *the percentage of information security incidents caused by improperly configured*

access control. An example that relies on information regarding efficiency is *the percentage of system components that undergo maintenance on schedule*. Effectiveness/efficiency measures can be used to improve the performance of information security programs.

Impact Measures Impact measures are about the impact information security has on an organization's mission. The use of impact measures will be different for different types of organizations. They can for example be used to quantify costs related to information security events, savings related to the information security program or the degree of public trust gained by the information security program. Impact measures combine information about resources with information about the results of security controls. An example of such a measure is *the percentage of the agency's information system budget devoted to information security*.

The guideline defines several considerations organizations should be aware of that can help make their programs successful. Some of these considerations will be discussed here. Organizations should include appropriate stakeholders in the development of information security measures and programs. It is important however, that each stakeholder is responsible for as few measures as possible. Organizations should prioritize a limited number of measurements, since resources are limited and the entire process must be manageable for the organization. If the organization has got any units responsible for performance measurement the information security measurement program should be coordinated with these. The data gathering and reporting must be clearly defined and should be standardized. This will facilitate the collection of valid data. Automated data collection is a way to achieve standardized data collection and reporting. Another benefit to this approach is that it minimizes the opportunities of human error. Information security measurement is something that should be used throughout the entire System Development Life Cycle (SDLC). This can help integrate information security into the system development effort.

The establishment and operation of an information security measurement program is guided by two processes, measures development and measures implementation. The measures development process includes finding appropriate measures for the organization. The measures implementation process is iterative and ensures that the aspects of information security that is being measured in a specific time period are appropriate. The first phase of the measures development process identifies relevant stakeholders and their interest in information security measurement. The stakehold-

ers should be included in the entire process in order to ensure a sense of ownership of the measures and to establish the concept of measures throughout the organization. The second phase identifies and documents information system security performance goals and objectives. These goals and objectives should be validated by the stakeholders. Phase three is about information security policies, guidelines and procedures review. It focuses on organization-specific information security practices. Phase four consists of a review of any existing measures and data repositories that can be used to derive measures data. The review could lead to applicable information being extracted and used to support measures development and data collection. Phases five, six and seven include the development of measures that track process implementation, effectiveness/efficiency and mission impact.

It is important to establish performance targets when defining information security measures. These targets establish benchmarks by which success is measured. For implementation measures these targets are set to 100 percent.

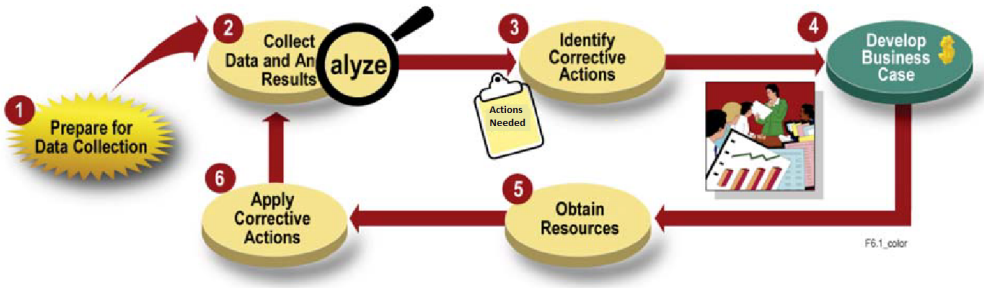

Figure 2.6: Information security measurement program implementation process [4]

The measures implementation process consists of six phases that is illustrated in Figure 2.6. The first phase includes activities like information security measures identification, definition, development and selection. The development of an information security measurement program implementation plan is also a part of this phase. This plan should define specific implementation steps based on how data should be collected, analysed and reported. The second phase ensures that measures are used to gain an understanding of information system security. It consists of a collection of data in accordance with the plan made in the first phase and an aggregation of measures to create higher-level measures in addition to an analysis of the

results. Phase three involves determining the range of corrective actions and a prioritization and selection of these corrective actions based on risk mitigation goals. Phases four and five will use results from the preceding phases to develop a business case. The business case is in turn used to develop a budget request. The sixth and last phase involves an implementation of corrective actions in the security program, or in the technical, management and operational areas of security controls.

A selection of the measures proposed in this guideline are described in section 2.2. These measures can be used as is, modified or used as template.

2.4 Related work

Tone Hoddø Bakås wrote a master's thesis about information security metrics in practice in 2005 [19]. Her research questions were about examining what characteristics companies and organizations that measure information security have and what good practice for measuring information security is. The latter includes what kind of methods are used, what the organizations' purposes of measuring information security are and what effect they claim it gives. The master's thesis also contributes with a proposal of a process for measuring information security.

That project was different form this project, in the sense that both research questions and methods are different. Hoddø Bakås used a questionnaire survey, with supplementary interviews of a selection of the participating organizations, as opposed to this study, where in-depth interviews are used. This study does not seek to find any differences or similarities between industries.

The results from the questionnaire survey suggested that some organizations measure information security to a greater extent than others. These are organizations that have partially outsourced IT systems, belong the financial or service industry, have an IT security manager, have 5 or more employees that work with security or are more concerned with measuring in general. The results also suggested that government-owned organizations measure information security to a lesser extent than other organizations.

The results showed something about what types of measurements for information security were performed. Organizations seemed to use several different methods for measurement. Many seemed to use methods they had

developed themselves and few seemed to use commercial products. Among methods used were measurements of incidents and security breaches and external audits. Most of the organizations used quantitative methods, some in a combination with qualitative methods. The results showed that the main reasons why organizations measure their information security were to communicate status to the management and to prove compliance with security standards.

2.5 Challenges related to security metrics

There are many challenges related to information security metrics, some of which are discussed throughout this chapter. One general challenge is that many security-related elements are vague and difficult to include in a meaningful measurement. Three such elements mentioned in [1] are asset value, threat and vulnerability. Asset value can to some extent be measured, for example if assets are actually compromised and are fully or partially useless for some period of time. Other aspects to asset value are harder to measure, like the organization's reputation. Some security measurements tend to become quite subjective.

Security metrics is not a mature area, and it can therefore be difficult for organizations to know how to manage it. [1]

Chapter 3

Method

This chapter describes the method used for collection of empirical data on how security metrics are used in various organizations today.

3.1 Method used

Face-to-face interviews were chosen as the method for this study. All of the interviews were performed by the author and there was one interviewee per organization. One interview was conducted per organization and a total of five organizations were interviewed over a period of four weeks. All of the interviews were voice recorded. The method used is a qualitative method [20] where relatively few informants were chosen. This allowed for a focus on in-depth information from a small number of organizations rather than less information from a larger number. With few informants the opportunity to generalize was not there, which it would have been if a quantitative method had been used. The type of interview chosen is somewhere between a structured and an unstructured interview and can be called a semi-structured interview. In semi-structured interviews an interview guide with some defined questions and themes is used, but with the possibility for clarification and follow-up questions that may arise during the interview. The order of the questions is determined by the conversation instead of being predetermined. The interview guide can be seen as an incomplete script [21]. The interview guide for this project can be found in Appendix B (in Norwegian).

The selection of organizations includes organizations of different sizes, from different industries and both private and government owned organizations.

3.1.1 Why this method

The main reason for choosing face-to-face interviews was that this gave the possibility to explain the questions in the case of any misunderstandings. It also gave the chance to come up with follow-up questions on the spot. Choosing this method included choosing to get fewer participants than if e.g. a questionnaire survey had been used. Even so this seemed like the best choice as I believed that interviews in general give more exhaustive answers and by that more and better data to work with. By recording the interviews I was able to concentrate on the dialogue instead of taking notes, and I was able to go back and go through the data several times as needed. This way I was also able to confirm or clarify things I was not sure of later.

A face-to-face interview is likely to be perceived as more personal and therefore it was assumed that this method would create more trust between the interviewer and the interviewee. When the interviewer actually shows up in person and there is a conversation, the probability of getting sincere answers may be higher than if a questionnaire survey is being used. By scheduling an interview it could be easier to get answers from the ones you hope to get answers from, a survey is easier to forget or ignore.

3.2 Ethics

This project could turn out to contain business sensitive information and there were therefore ethical aspects to consider. It was assumed that businesses would not want their security policies and metrics methods publicly exposed. Another important aspect to consider was that even though the questions were about the organizations, the privacy of the interviewees is important. The interviews were taped and voices could be recognized if someone were to listen to them. Because of these issues it was important that they should know beforehand exactly what they were participating in. Therefore all participants were given an information sheet and were asked to sign a statement of consent. The project was also reported to the Norwegian Social Science Data Services. The information

sheet and statement of consent can be found in Appendix A (in Norwegian). It states, among other things, that any participant can withdraw from the study at any time, at which their contribution would be removed from the study.

Another aspect considered beforehand was that the author might have to sign a confidentiality agreement before performing the interviews. There was however none of the interviewees that mentioned such an agreement and it seemed like the anonymization was enough.

3.2.1 Anonymization

No individuals or individual organizations have been mentioned in this report. All organizations have been given pseudonyms, so their entire participation in the study is not publicly known. Any relation between individual organizations and results has been anonymized at the end of the study, and only available to the author and partly her supervisors. The term anonymized means that any information that could directly identify individuals or individual organizations is deleted and that any information that could indirectly identify individuals or individual organizations is deleted or changed.

At the end of the study all recorded interviews will be deleted. This means that the recordings will not be saved and hence only used as a basis for this report and one scientific paper based on this study.

3.3 Challenges

Preparing and performing semi-structured interviews can be very challenging especially if the interviewer does not have any experience when it comes to interviewing people. A questionnaire survey could have been easier, given my experience, as this allows all questions to be defined beforehand and there is no room for improvisation. On the other hand it can be challenging to construct unambiguous questions and questions that will give all the data needed. In the case of a questionnaire survey there is no opportunity to elaborate questions if misunderstandings arise. Michael D. Myers and Michael Newman discusses some potential problems to qualitative interviews in [21]. They mention that the interview can become artificial as it is usually

two strangers meeting where one of them has to give opinions within a limited amount of time. This limited amount of time could cause the data gathering to become incomplete or it could force someone to create opinions under time pressure when these opinions were not held strongly to begin with. I tried to avoid the problem related to time by setting aside more than enough time for each interview. Another problem mentioned is lack of trust. The interviewee may in some cases be reluctant to reveal information regarded as sensitive, either related to themselves or the organization they are associated with. It is difficult to overcome this if it should arise, but it is sensible to assume that by reporting the project to the Norwegian Social Science Data Services and informing all interviewees about how the information they share will be anonymized, the probability of getting truthful and complete answers will increase. Another problem is that an interviewer may actually cause knowledge to be constructed as the interviewee may try to answer something he has not thought about before, but he wants to appear knowledgeable and rational so he constructs a story. Despite these challenges, given the previously discussed advantages to this method, this method seemed like the best choice for this study.

Chapter 4

Results

This chapter presents the results from interviews of five organizations with different core operations and of different size. Table 4.1 shows the definitions used in this report to define the size of the interviewed organizations.

Number of employees	Size of organization
$<$ 20	Small
20 - 100	Medium sized
$>$ 100	Large

Table 4.1: Size definitions of organizations in Norway, derived from [22]

The organizations interviewed are classified by using these definitions for sizes and by dividing them between privately owned and government-owned organizations. The term government-owned organization is in this report used to refer to an organization that to some extent performs operations on behalf of the government and not a commercial organization where the government happens to own parts of, or the whole organization. Table 4.2 shows an overview of the interviewed organizations.

Organization pseudonym	Size of company	Type of organization
Organization A	medium	private
Organization B	large	government-owned
Organization C	large	government-owned
Organization D	medium/large [1]	private
Organization E	large	government-owned

Table 4.2: Size and type of companies interviewed

[1] This organization is a subsidiary of a larger organization and the total number of users corresponds to a large organization.

4.1 Organization A

This section describes the results from the interview with Organization A.

4.1.1 The organization

Organization A is classified as a medium sized organization. It is an IT-consultant company and its functions consist of delivering IT-solutions to other organizations. The interviewee was the IT security manager. The organization is to a very large degree dependent on IT.

The IT operations[1] of the organization, like server hosting, are mostly done by the organization themselves, but a small part is being outsourced. The employees use certain external web-based services in their daily work and these are services that the organization cannot control.

The organization owns a lot of documents that are business sensitive, like templates for project proposals[2]. When documents are business sensitive they include information that the organization does not want their competitors to gain access to. The quality and content of these documents are what

[1] The term IT operations is in this report used to describe processes and services used by the organization itself or by an external party to run the organization as a business. This definition is derived from Wikipedia's definition [23].

[2] A project proposal is a document containing a proposal for how the organization can perform a specific project. The purpose of the document is to sell their organization's or their employees' services to a potential customer who needs someone to perform a specific project for them.

decide whether or not they will be able to sign any new contracts and are therefore crucial for the organization.

The organization has one customer that generates a large part of their revenue, and it is very important to maintain a good relationship with this customer. It is important for the management to know that the security related to this customer is sufficient. This is important to avoid distrust between the two parties, and this is something the management would want to know. In order to keep the customer's trust they need to be able to show them that their security is in fact good enough. The organization has access to the customer's network from their offices. This access is granted as long as they fulfil a set of requirements.

4.1.2 Measurements and reports related to security

When it comes to systems the organization has purchased the IT security manager has conducted a risk assessment prior to purchasing them. For some systems the risk assessment was conducted after the system was purchased. This happened because someone bought it without consulting the IT security manager beforehand. The risk assessment is done several times in order to be able to continuously evaluate the security of the systems. There is an employee that is responsible for each system. This is typically someone who uses this system in his or her daily job. This person is also informed about the procedure related to the risk assessment. The risk assessment consists of a review of the systems confidentiality, integrity and availability.

The IT security manager annually writes a report related to the security in the organization. This report lists what security measures, i.e. what actions related to security, have been done, what incidents have happened and what actions were taken in response to these incidents. The report includes what potential for improvement the organization has, when it comes to information security. The goal of the report is to give the management an overview of the organization's situation and to learn something from what they have experienced. It is also used to plan what actions should be taken the following year.

All incidents that are in a way reported to the IT security manager are measured, but this only includes incidents that are concrete and have led to a security breach. The organization gives the opportunity to use Jira[3] as a

[3]Jira is a project tracker that includes functionality for reporting issues [24].

system for reporting of incidents. It has yet to be used by anyone though, and all reporting is in practice done by reporting directly to the IT security manager. Their security policy says that you can choose between using Jira, reporting to your closest manager or reporting to the IT security manager if you suspect a security incident to have happened.

The IT security manager discovered that the employees did not take good care of documents containing sensitive information. These documents were often copied to unencrypted USB-sticks and taken out of the premises of the organization or sent by email without any additional means to secure the information. In many cases this was done due to specific demands from the customer. In relation to this he stated:

> *"The most critical information we had was the information that was the least taken care of."*

4.1.3 Use of results

The risk assessment of the outsourced systems was used to figure out if the supplier could be trusted to deliver a sufficiently secure system. If they saw that the risk was too high, changes in the contract with the supplier were made or they made sure that there were changes in the use of the system.

The annual report written by the IT security manager is presented for the board[4]. He feels that the managers think it is useful to get this report because it is a way of informing them about the status of the organization's information security. If the incidents are serious the management is informed about them when they actually happen, but otherwise the report is where they get this kind of information. The interviewee thinks that the reports are useful for the management in the sense that they can learn something about it. This is particularly applicable when it comes to the management understanding more about trusting third-party suppliers. As the management are often not the most technically skilled employees, they often need to get these issues explained in way that they can understand and sometimes they need to be reminded about issues related to security. It is very useful for the management to get reports about the status of the security in the organization, because they can then use this report to

[4]The board consists of both external and internal participants.

maintain their relationship with all their customers, especially their largest customer.

For some incidents several people participated in the review, typically including those who were involved. In some cases the incidents were only reviewed with the ones involved. Subsequently they had a general review about the cause of the incident as well as actions that can be taken to prevent further similar incidents. These sessions were conducted involving several people. By doing this, incidents are used to increase awareness and knowledge about security in the organization, without necessarily having to talk directly about a specific incident and without letting everyone know who was responsible for a security breach.

The result of the measurement of incidents are not really compared to anything, but if they seem to be much deviated from previous results they take this as a sign that something is not the way it should be. An example is that they had registered few incidents this year. They took this deviation as a sign that there could be incidents they had not yet discovered, because they had no reason to believe that they should have had fewer incidents this year.

After observing that important documents were not very well taken care of they tried to teach the employees, and subsequently their customers, about what methods for transferring information are secure and which methods they should and should not use.

The IT security manager does not feel that the measurements they perform demand a lot of extra work. The IT operations department does the measurement of incidents and the report that he writes himself is not something that he spends a lot of time on. What does require extra work however is the actions that have to be taken after an incident has happened. As this is not a very large organization and as it consists of people who are more skilled with computers than most organizations, he thinks the security is easier to manage. As their employees are computer skilled they may not require as much training as others when it comes to security, but at the same time they could be able to cause damage in ways less skilled employees would not have been able to do. This damage is not necessarily caused because they have bad intentions, but because they perform certain tasks most employees in other types of organizations would not have performed. This makes the security challenges a bit different for this organization than for many others.

The IT security manager can see that a best practice for security metrics could be useful, but that a standard may not be suitable for their organization. The reason for this is that a standard often has certain constraints that do not fit well with their organization.

He thinks it is difficult to say if their way of measuring security is good enough. He does however emphasize that there are perhaps not so many serious threats towards their organization. He does not see their organization as a very attractive target compared to many other organizations.

They monitor all servers and systems, and thus probably have other data that they could have used for measuring security, but he thinks it is important to consider the employees' privacy when considering what data to use for measurements.

4.2 Organization B

This section describes the results from the interview with Organization B.

4.2.1 The organization

Organization B is a governmental agency. The users of their systems are located at several places in the country. The interviewee has the responsibility for information security and IT strategy in the organization. This responsibility includes the introduction and development of IT management systems.

They are currently in the process of renewing their IT systems. This is a large project that has duration of about four years and it involves large changes. The basis for this project was an analysis of their current systems that showed that these were quite diversified and some of the systems were not even well correlated to the work process. There were also security related problems with the old systems. Through the years, systems have been developed as needed and this was probably one of the reasons for the diversification. Another reason for the need for new systems was that the organization got new tasks to perform. As a part of the renewal they have built better systems for security.

The development of the new systems is mainly done by external parties, but under the management of employees in the organization. One of the systems is being both developed and managed externally. Their IT operations are currently outsourced as a trial project. The supplier of the IT operations is responsible for keeping firewalls and programs, like antivirus, up to date.

Organization B is completely dependent on having good IT solutions when performing their operations. They also depend on their systems operating at different locations to be able to communicate.

They have data that are very sensitive and it is crucial that these data are not exposed to someone who is not authorized. Information security is therefore very important for this organization. There are few technologists in the organization and thus the knowledge about information security may not be very high, at least not compared to organizations with more technologists.

4.2.2 Measurements and reports related to security

When it comes to measurements related to information security this organization characterize itself as being in an initial phase.

"Do we perform any measurements related to security? No"

A year ago an external party audited the information security in the organization. This audit revealed several issues that needed to be improved. One of the things mentioned was that they did not have an Information Security Management System (ISMS). The actions taken to ensure secure systems were more or less random and based on the developers' knowledge.

The supplier of their IT operations is responsible for all surveillance. They report incidents, like intrusion attempts, to the organization. Even though they have these reports, the selection of issues reported is neither thoroughly considered nor holistic. These reports are delivered either each week or each month.

The organization uses a system for reporting nonconformities. This system can be used for reporting of information security related incidents.

4.2.3 Use of results

Part of the results of the audit of the information security was known to the organization beforehand, but this audit gave extra incentives to actually do something about it and to actually make the necessary investments. Before the audit, the argument for not doing anything about their problems was that they did not have enough resources. As a result of this audit they have started to develop an ISMS based on ISO/IEC 27001 and ISO/IEC 27002. They have mainly focused on ISO/IEC 27002, which presents 133 security controls.

They have chosen the controls that were the most important and most relevant for their organization to be included in the first version of their ISMS.

The model they have developed does contain something about security metrics, but not specifically which metrics that should be used. This model is a first version, meaning that it is supposed to be changed and further developed. This is in accordance with ISO/IEC 27001 [17]. By doing it this way they get a partial ISMS relatively fast instead of spending many years on developing a complete one before being able to put any of it into operation. The ISMS is built such that decisions are supposed to be taken in the strategic parts of the organization and by the people who own the work processes. They have identified unwanted incidents through a classification and risk analysis. This is transferred to the technical domain of the organization by identifying actions towards the unwanted incidents.

An important aspect of their ISMS is an annual report to the management. This report summarizes the security condition of the organization. It is supposed to give the management a basis for making necessary decisions. It is important that the CEO is a part of this, as he/she is the one responsible if any laws have been broken, for example if any sensitive information is stolen. It is also important that critical issues and questions are presented to the management, as they are often the ones who have to make the decisions. Partly because those decisions may have economic consequences as they may involve investments. The report highlights these questions. The annual[5] report is something that is specified in ISO/IEC 27001 [17].

[5]The standard specifies that the management must review the organization's ISMS *at least* once a year

The interviewee thinks that the use of results from measurements for an improvement of knowledge must be part of the point of doing the measurements in the first place, but emphasizes that the results must be "translated" so the management can understand it. It is also important not to present everything, but to choose the relevant parts.

Their current ISMS's primary functions are to introduce a classification and risk assessments of their systems in addition to setting requirements for the development of new systems. The classification aims at placing systems in security classes where each class has requirements and potentially options. In practice, this is done by a consideration of the information contained in each system and a classification of the system based on how sensitive this information is. This approach is chosen rather than e.g. concentrating on which technologies are being used. By doing this they hope that more people in the organization will understand why information security is important and that it is not about technology, but about the information. All the systems or processes have an owner, and they are not necessarily technologists. These people participate in the classification process, and this contributes to an increase in their security awareness. By focusing on the information in the system it is easier for non-technologists to understand the problem. When the classification was established they could move on to the risk analysis where they identify the worst-case scenarios and subsequently define concrete actions that should be taken to prevent this. In this last part the technologists are involved.

The reports from the supplier of their IT operations are not connected to their ISMS. It is the IT department of the organization that receives these reports and they are not really presented for anyone else, like the management.

If someone uses the system for reporting nonconformities the IT department processes these reports. There are currently no procedures for reporting this further on to the management.

4.2.4 Plans for the introduction of information security metrics

They plan to use what they have already introduced in their ISMS as a basis for the establishment of measurement parameters. They will focus especially on the transfer from strategy to technology. When they have introduced

the desired security controls they aim to introduce security metrics and measurements. It was the interviewee that initiated this process.

They have not yet used ISO/IEC 27004, which addresses measurement of security, specifically measurements to assess the effectiveness of their implemented ISMS and controls or groups of controls.

They plan to have regular meetings with the supplier of the IT operations where the supplier reports on previously stated parameters. These meetings will also be the arena where they discuss necessary actions related to the security in the outsourced systems. The reports from the supplier are also supposed to be presented for the management in the organization, as part of the summary of the security condition. The interviewee feels that their prior work with the classification of their systems has led to increased security awareness in the organization and that this will contribute to making it easier to introduce measurement parameters.

One of the main reasons for introducing information security metrics in the organization is that this will give an indication of the security, where they stand. Another important reason is that by choosing the right metrics, the management can also get an understanding for the necessary actions related to security. The interviewee summarized this in the following way:

> *"It is important to have measurements to know where you stand. The other thing is that if you measure something that is reasonable and that system owners and management care about and understand, you can get a collective understanding of the wish to initiate actions."*

The interviewee thinks that government-owned organizations have a different focus than a private organization. The main difference is that their systems are not related to any income as they often are in private organizations. Their largest concern is their reputation and if they do not have secure systems, this reputation will be damaged, especially since they process such sensitive information.

The interviewee believes that to be able to measure security you need to have a structure or an ISMS. This ISMS can create a basis for the introduction of information security metrics, and thus make this introduction easier than it would have been if you started out with trying to define the metrics. This way one can connect metrics to mechanisms already in use in the organization. He also believes that a best demonstrated practice would be very useful. In

addition they have experienced that organizations are quite good at sharing their experiences regarding IT and information security. The interviewee feels that this has been very useful for him and the organization.

4.3 Organization C

This section describes the results from the interview with Organization C.

4.3.1 The organization

Organization C is government-owned and their systems have a large amount of users. The interviewee is the IT security manager. His responsibilities include concrete technical actions related to security as well as the development of guidelines regarding the information they process. The users of their systems have different roles and these roles determine which access rights each user has and which systems he may use. Their basis systems are a personnel and salary system, a financial management system, a system for archiving and an email system. They also have integration with an external system. For some of the users, this is where their identity is established. For employees their identity is established in the personnel and salary system. In addition to the mentioned systems they have a system for the distribution of identities to all of their other systems. This organization is dependent on IT to a very large degree. Most operations could not be performed without it.

The IT operations of the organization are for the most part done by the organization itself. However, they have to a larger degree started to outsource parts of their IT operations.

They have a large amount of sensitive data and it is important that these are properly secured. The handling of these data is something they take care of themselves. It is important both for their users and for their general reputation that the security in the organization is well taken care of.

They have a security policy and a number of principles related to that policy that is applicable to all of their systems. This policy includes descriptions of how they are supposed to manage their information and the various user roles. Each system has a system owner in addition to someone who

is responsible for the system. The system owner is typically someone who works in the department that uses the system and the one responsible for the system is often someone from the IT department.

This organization has based its information security policy on ISO/IEC 27001 and ISO/IEC 27002. Among other things these standards include guidelines to be used before the acquisition or development of a new IT system. They have to ask themselves questions, like what the system will be used for, what data it will contain, if that data are static or dynamic and what other systems it needs to be integrated with. Subsequently they create a risk matrix for the system to find what kind of level of security the system needs. From there on they can find security actions that need to be performed. The organization is not certified, but it is in compliance with the standards. They do not use ISO/IEC 27004, which involves measurement of security.

4.3.2 Measurements and reports related to security

The measurements they perform are mainly related to audits of their systems. One form for audit that they have done involves penetration tests of systems. They perform penetration tests of new systems, before they are deployed, but they also test systems that are in use and these tests are part of the audits the organization performs.

Another form for audits concentrates on the information part of the system, rather than the technical. The interviewee describes this as being more difficult than the technical audits, where they can perform penetration tests. In the audits that deal with information they talk to the users of the systems. They ask questions about how these users treat sensitive information in the systems, e.g. how they exchange information.

In addition to the internal audits, there is an external party that audits their systems. This is in relation to the organization being a government-owned organization. This audit involves checking how they take care of their information and how they spend their money. There are also other external parties that control organization C, and they are among other things, interested in how they perform their own audits. Before performing these audits they spend time on explaining the users of the systems why they need to do it and they also involve them in the auditing process itself. The goal of doing this is that it will lead to a better understanding of the

importance of securing information.

There is an external party that performs an open threat assessment each year and this year it concerned several areas relevant to Organization C. The assessment mentioned several of these areas as being interesting as potential targets for adversaries. Due to that threat assessment the organization has decided to start an audit concerning systems used in these areas. The audit will involve interviews with users of these systems, and the goal is to reveal the users' relationship to information that they process in their daily operations. In addition the organization will try to reveal what these users think about the security around this information, specifically how they think it is secured and what they think the requirements are. Subsequently the audit will contain an identification of the actual requirements and a comparison to reveal any potential mismatches.

Organization C also measures incidents. The IT security manager receives reports three times each day concerning security events and also information about which clients have the most outbound connections. He receives firewall reports, including information on IP addresses that conduct port scanning towards the organization's networks. These are reactive measurements, but it has shown to be effective as incidents are discovered relatively fast.

They have tools that automatically search through their systems for old versions of operative systems and applications. However they do not produce many concrete numbers related to these searches. The interviewee reflected over in which sense this was a measurement or not. He concluded that it was not in the sense that you measure something and get a concrete result but in the sense that you perform a measurement, find any deviations, implement countermeasures and perform a quality assurance in retrospect. In general he would prefer measurements to be concrete, and stated:

> *"My experience is that, at least when it comes to technical aspects, it is a lot easier to deal with concrete things."*

Information security is, as mentioned, very important for this organization and the potential consequences of a security breach are the reasons why they initiate the actions they do to try to keep their systems secure. The measurements they perform are a part of this.

When it comes to the outsourced systems they have requirements regarding how their data should be treated. As a part of these requirements they have stated that they should be able to check how the supplier audits the

systems whenever they want to.

Each year they have to deliver a report to a ministry that allocates them money in accordance with predefined specifications related to the use of this money. In this report they have to show that they have used the money as specified by the document. One part of this document specifies reporting of information security.

The interviewee specifies that he thinks that there are potential gains in measuring security. He thinks that these measurements are in general proactive and if you reveal weaknesses through a measurement process, instead of when a security breach has happened, the costs will be much lower. In spite of this, he thinks it is difficult to "prove" this to the ones who make decisions regarding investments, as it is difficult to show how much you have saved on certain actions to secure your systems. He does not feel that it demands any extra amount of work, as he sees this as being a part of each system's life cycle. A functioning system must be audited and improved.

They have a system for reporting of incidents and nonconformities. This system can be used for reporting of information security related incidents. The goal of this system is to be able to learn from previous incidents. Today the IT security manager is not the one who directly gets reports related to information security, but he wishes to change this and that the system should be used more broadly. In practice a large part of this reporting is instead done internally in the various departments and reported to the IT security manager if they see the need for that. There is also an email-address where people can report incidents. The emails sent to this address are mostly generic questions or concerns, but they can still reveal potential issues. The interviewee specified that he believes that there are many incidents that are not reported.

4.3.3 Use of results

The results of the audits that concentrate on information are compared to their routines concerning information security and the treatment of sensitive information. In specifics, they look for deviations in the practice when compared to their routines and policies.

When someone has discovered an incident or a deviation from what is normal, they report this to the IT security manager. In this case there are concrete

issues that are reported, or revealed after the initial report. This can be how long a security hole remained open, what data was lost or in some cases who it was that broke into their systems. These measurements are defined by the interviewee as being *reactive*. The other type is *proactive*, and the proactive measurements they perform are the audits of their systems. Large, serious incidents are evaluated in retrospect. They are also categorized and included in the annual report to their superior ministry.

Before audits are performed the system owner gets an explanation of the audit. The reason for this is that if they discover something that needs to be changed it is the system owner who is responsible for doing this.

The audits are also discussed in an information security forum where the status of the different systems is reported. This way the IT security manager gets an overview of the overall status. The audits can also be used to compare departments to see if there are any differences. In performing such a comparison it is important to consider whether or not departments are really comparable. It would for example be sensible to compare departments with the same level of sensitive information. On the other hand it is not useful to compare departments that are totally different as they have different requirements regarding information security.

The users of the different systems are involved in the processes of coming up with proper actions related to the results of the audits. By involving them in the entire process the IT security manager hopes to make them understand that information security is important for them to consider as well. They are the owners of the information and they will suffer in the event of a loss of information. He also thinks that they will increase their trust in the systems they use, as they learn more about how the systems work and how they are secured.

The interviewee wishes that they used metrics that were more proactive and that could give more concrete results. This could lead to a more systematic approach for measurement of information security. It would also be useful for him to have more human resources to involve in the process, as now he has got practically the entire responsibility himself. He would also have liked to have someone to evaluate him, because currently he has to both make the requirements and verify that they are followed in practice.

The interviewee thinks that if government-owned organizations were required to be ISO-certified, both ISO/IEC 27001, ISO/IEC 27002 and eventually ISO/IEC 27004, this would make it easier for them to measure security. If

it is not required it is easy to prioritize to spend the money elsewhere. The general idea is that it should come "from the top" i.e. from the management, because they have to accept the actions related to information security metrics before they can be performed. He thinks that a standard regarding metrics could be useful, but emphasizes that it must be general enough to be useful for any type of organization. In relation to this he could see the use of an appendix to the standard with a number of approaches where organizations can choose the ones relevant for them.

4.4 Organization D

This section describes the results from the interview with Organization D.

4.4.1 The organization

Organization D is a private organization. This organization is a subsidiary of a larger organization and their main operation is to take care of the IT functions for this larger organization. The interviewee is the ICT manager, who has the responsibility for quality and security. He is the only one in the organization that works with information security, except in cases were he asks e.g. someone from IT operations to perform certain tasks. Their main system is an ERP[6] system. This system supports their main operations. It also has integration with other systems they use. They are 100% dependant on IT as it is a part of all of their operations.

They do most of their IT operations themselves but parts of the IT operations are outsourced. They have developed a security policy in accordance with ISO/IEC 27001 and ISO/IEC 27002. The organization processes sensitive information, especially information about the employees.

[6]ERP stands for Enterprise Resource Planning and is an integration of business management practices and technology [25]. An ERP system is a system that supports coordination of different actors in a company. It can contain modules for any function that supports business operations. [26]

4.4.2 Measurements and reports related to security

They have bought an IDS from an external party and they receive monthly reports from them. They are additionally notified if something unusual happens. The IDS reports can say something about how often the laptops that move between their own and other networks are infected. Many of these laptops are used both inside and outside Organization D's firewall.

The organization generates reports regarding firewalls, event logs in Windows, antivirus and access control. All of these reports are delivered monthly. The reports regarding antivirus give information about the extent to which computers and servers have been updated with the latest patches. The patching is an automated process, but it does not always work. All of their systems generate reports, and the challenge they are faced with is that it is too much data. It becomes difficult to know where to begin and what to focus on. Now they focus on systems where they have seen that they have errors or viruses.

They perform these measurements to reveal what is going on in their systems. If they had not performed any measurements they would not have known this. In the case where no measurements are performed it is difficult to know if the systems work the way they are supposed to. The initiator of the measurements was the IT operations department.

They have audits for both their internal systems and the outsourced systems, meaning that all of their systems are audited. External auditors do both of these audits once a year. The outsourced systems are especially thoroughly audited every second year, involving a visit to their premises. In the audit of their internal systems the auditors compare the organization's practices to the ISO/IEC 27001 and ISO/IEC 27002 standards. The audit of the outsourced systems can contain penetration tests. They also perform penetration tests of other systems.

They have routines for reporting of incidents, if someone suspects that something has happened. The challenge here is that people often do not know that an incident has occurred, hence these reports are rarely sent. They have a separate routine for incidents regarding employees, i.e. if someone suspects someone else to have done something. In this case they have to fill out a specific form. For other incidents the routine involves reporting to their service desk.

There have been requests for reports regarding access to sensitive information

about employees. Specifically there has been a wish to know who has access and who has actually accessed this information. This is something they are trying to solve, but there is a question about investments involved.

The interviewee thinks the question about gains or worth of measurements and reporting versus the costs of it is difficult. He says that it is like insurance and it is difficult to know how much you should invest in insurance. Now they have chosen actions and measurements that are quite basic. These are actions and measurements that they feel like they have to have, and that everyone else has as well. Any further investments must be evaluated. In the case if this organization, it is the larger organization that they are the subsidiary of that makes these choices.

The interviewee thinks that a standard for metrics would be useful, because this lets you benefit from something others have experienced and found out. They have not yet used any such standard. He thinks the challenge with such a standard is that they are usually large, so you have to be able to choose the parts you feel are relevant for your organization. Such a standard would be a good place to start.

4.4.3 Use of results

The main way of evaluating any results from measurements that they use is a comparison with previous results. They use deviations to examine if something unusual has happened and in that case they try to find out what that was. It is difficult to go through absolutely everything and therefore they have chosen this approach. The interviewee does not think the measurements require a lot of extra work, but the process of following them up does.

The IDS reports are used to evaluate whether or not they should force all laptops to connect to the Internet through their organization's own network. If they see that many laptops get infected outside their firewall, they can use this to justify the investment that is required if this action is to be taken.

When it comes to the firewall reports they go through them and compare them to previous reports to see if something new or unusual has happened in their network. The same goes for the reports regarding event logs, antivirus and access control. Organization D has a security forum. In this forum reports about security incidents are discussed, including the

reports mentioned above. They discuss if the results are what they expected or if they have to take a closer look at them. There are five people who participate in this forum. This is the ICT manager (the interviewee) and people from the IT operations department. Half of the group is part of the management in the organization. They have meetings once a month. Further reporting to the management is not usually done; the exception is if something special or very unusual happens.

Included in the audits is a part where they compare the results with the results from the previous years, to find out what has changed. The auditors explain best practice and ask questions regarding how the organization complies to that and in some cases why it does not. The audits also include a comparison with other organizations and this can be used by Organization D to find out where they stand relative to others. They find these audits useful and feel that this is the type of measurement that works the best, because an external party tells them what they need to do better. This can sometimes be difficult to see for yourself.

The results of the penetration tests are compared to previous results and presented for the management. The reason for this is that these results say something about the quality of what they have developed. The results of the audits are also reported to the management.

Results from audits regarding access control have been discussed with several employees, because the results showed that administrator users were used at times when they were not supposed to.

If the audit reveals any nonconformity from the policy the auditors make some requirements to the organization. In this case it is a given that they will have to follow these requirements and therefore they do not have to make an assessment of the cost versus the benefit.

They do not have any means of correlating logs and reports from various systems and the interviewee believes that they would have been able to reveal more security related problems if they had been able to do this. This is something that they wish to improve along with creating even more logs than they have now. The main thing they wish to improve is the correlation of different log data, as a large amount of data is practically useless if it cannot be used for something sensible. Another challenge they are faced with is false positives. There are many incidents that are logged that are not really interesting and sometimes they might end up wasting time on these incidents instead of something that is actually interesting.

The interviewee explains that in Norway, the group of people that works with information security is small and that there exist several arenas where they meet and get the chance to discuss information security. They do not directly talk about or compare results from measurements, but they discuss challenges, among other things, revealed by these measurements. This way they can help each other to improve their practices and share experiences.

4.5 Organization E

This section describes the results from the interview with Organization E.

4.5.1 The organization

Organization E is a government-owned organization and their systems have a large number of users. The interviewee is the security manager in addition to being responsible for the IT department of a regional office. This organization is completely dependent on their IT systems. They have become more dependent during the last years and have been able to reduce the number of employees due to increased effectiveness in their IT systems. They have a large amount of sensitive data, so information security is very important. Their IT operations are outsourced. This includes, among other things, their IDS, firewall and antivirus. Organization E demands that the suppliers of their IT operations are ISO certified.

They have during the last years developed an ISMS that involves six fixed activities each year. They have used the ISO/IEC 27000 family of standards, but they have not yet used ISO/IEC 27004.

4.5.2 Measurements and reports related to security

They monitor their systems and they generate monthly reports related to most of their IT operations, like their IDS, firewall, virus and deployment of updates. The supplier of their IT operations reports to them when something happens. This involves measuring the number of incidents. This

supplier also reports how many clients that have been infected by a virus and how many have been quarantined.

Each year risk assessments of their systems are performed. These risk assessments are both performed for each area of operation and for changes in systems. They perform their risk assessments based on the method described in ISO/IEC 27005 [27].

The activities related to the ISMS usually result in reports. Each year they have a review of their firewall rules. For each change related to these rules they have a control loop. They log most events in their systems, because they need to have full traceability in the case of errors. Therefore they might have additional data that could have been used to measure security.

An external auditor audits them once each year. This audit is related to their ISMS and checks whether they are compliant with the standards that they use. The main purpose of the audit is to reveal issues that were not focused on in the implementation of the systems.

They perform security tests of their infrastructure periodically. There is an external party that performs these tests, as there should be someone else than the organization itself that evaluate their security. These tests often reveal issues that need improvement.

The main goal for performing measurements is to get a certain level of control. In addition there are certain numbers that a security manager needs for reporting to the management to get (and keep) a focus on security. This is needed in order to be able to show them what has happened. The existence of incidents and other issues related to security are not obvious to everyone. Therefore the management needs to get results presented to them so that they can understand that it is in fact important to focus on security. Another aspect of these measurements is that they want to be able to discover and avert any incidents. Related to measurement of information security, the interviewee stated:

> *"There is no good definition of what measurement of security really is. Where are you on a scale from something to something else? You count many things and have a gut feeling as to where you stand"*

Currently they do not have any high costs related to measurements of security, because they only measure on the level that they "have to" measure. It is mentioned that it is difficult to measure security:

> *"When it comes to performing more widespread measurements of security. It's that hard thing about security. You try to avoid certain things from happening, and then security becomes very difficult to measure. You only say that it is a good thing that something didn't happen... It is hard."*

They have a system for reporting of incidents and nonconformities. They have chosen to use this existing system for information security related incidents as well. The external IT operations suppliers have their own systems for reporting. In their security policy they have defined that one should notify the closest manager if one suspects any incidents to have happened. Often the security manager is the one that is being notified. Subsequently the one being notified has to check if there really has been an incident and if so create a report in the system. They have in some cases experienced that after awareness campaigns people have become a bit too paranoid and several such notifications have not really been anything serious.

They are in the process of learning how to do measurements related to security, and it remains to be seen if what they have implemented so far works well.

The interviewee thinks that to make it easier for government-owned organizations to measure security, it needs to be a requirement. Most government-owned organizations are controlled centrally and therefore they do what someone else tells them to do. Measuring security is not yet one such prioritized and required activity. Until it becomes prioritized Organization E will probably not measure any more than they do today, but this is still more than they did a few years ago.

The interviewee thinks that a standard that says how one could measure security would be very useful. One reason for this is that it is a vague subject and without a standard it is hard to know what to do and how to do it. She also thinks that the standard should come along with some tools and specifies that both the standard and the tools need to be quite concrete. She emphasizes that one needs to be measured on this as well, i.e. if one is in fact in compliance with the standard. She believes that the challenge would be to get the standard concrete enough.

4.5.3 Use of results

The results from the measurements they perform are used to plan what they should focus more on than before. The results show where improvements are needed.

They have a year-to-year plan that involves activities for all the employees to increase awareness regarding information security. They choose the topics for these activities based on what they have seen that the employees need to be reminded of. They hope that this is useful for them and will lead to the employees thinking more about security. It is also mentioned that it may be useful for them in their personal life, and not only for work.

They use their risk assessments to try to find a security focus area for that year. They also have a discussion involving the management that contributes to finding this focus area. It also raises awareness in the sense that people start to think more about the issues that are discussed.

Once each year the management gets a report involving the measurements the organization performs. In the report they compare their results to large known statistics, from among others Symantec[7] and NSM NorCERT[8]. These statistics include the number of incidents that organizations are exposed to. This is useful for Organization E, because they have not been exposed to many incidents themselves. They do not have a lot of experience in this area yet, and therefore they do not have so much data themselves that they can compare their results to. As Organization E has not experienced any serious security breaches themselves this comparison is used to show the management that incidents actually do happen and that it is important to focus on security, even if it seems like they have not had so many issues related to security themselves. This way the management can get an understanding of the need to continue to invest in security related actions. As they develop more experience and get more data themselves they will begin to compare results with results from previous years.

The results from the tests of their infrastructure are also presented for the

[7] Symantec is a large international organization that provides security, storage and system management [28].

[8] NorCERT is the Norwegian Computer Emergency Response Team and is a department of the NSM, which is the Norwegian National Security Authority. NorCERT's tasks include gathering information related to serious IT security breaches, coordinating responses to such breaches, coordinating patches of vulnerabilities and sharing information regarding threats. [29]

management. As these tests often reveal issues, they are often granted money to implement actions to fix these issues.

Chapter 5

Discussion

This chapter contains a discussion of the results from the interviews with the organizations. Specifically the practices of the organizations is discussed relative to existing standards and literature about information security metrics. The chapter consists of an individual discussion of each organization. Additionally there is a discussion of the applicability of the metrics described in section 2.2.

5.1 Organization A

Organization A does not really have a system for measuring information security. It is a medium sized organization and thus may not need a large system for this either. They conduct risk assessments of the outsourced systems, but without calling this an information security metric, which is a good thing as this is not recommended as described in section 2.2.1. The organization measures the number of incidents, but without having a process related to the measurement and analysis it cannot be defined as being a metric. They do however use some of the results to increase knowledge and awareness related to information security, which is consistent with what should be the goal of metrics. They also compare the results implicitly to previous results as they use deviations as an indication that something is wrong. It seems that most of the activities related to the assessment of the information security condition are quite qualitative. They seem to be based on what is perceived as being current needs, and not

systematized or necessarily repeated. An example is when the IT security manager discovered that they did not take good care of the information they process.

Most literature related to information security metrics emphasizes that the management should play an important role in the measurement process. This is because they are the ones making the decisions in the organization. In organization A the management has only been involved through the reports they get presented, but the interviewee stated that when it comes to making necessary information security investments there has not been a problem to get the management's approval. The report presented for the management is used to increase knowledge and awareness within the management, which is compliant with existing theory. The management involvement in this organization may not be as important as it is in other organizations, as this is a medium sized organization with a quite flat structure. The report explains the general information security status is the organization, but apart from including incidents it is not related to measuring activities.

ISO/IEC 27004 states that the size, complexity and the role of information security in the organization should contribute to determine what kind of measurements they should use. The interviewee emphasized that the size and type of organization affect their choices related to information security. This organization does not really use any of the metrics described in chapter 2 and does not have an ISMS. In addition they do not do many quantitative measurements. They do therefore not comply so well with any described standards.

Organization A might benefit from measuring information security to a larger extent than they do today, but due to the size and nature of the organization a very extensive program from measurement would not necessarily be beneficial.

5.2 Organization B

Organization B is a large government-owned organization. They have outsourced their IT operations, but do not have any systematic measurements related to this. The supplier reports incidents, but there is no system around these reports either.

They are currently in the process of implementing an ISMS and they do

this part by part, to avoid spending several years before anything new is deployed. That approach also applies to their introduction of measurements. This is compliant to recommendations from literature, like the ISO/IEC 27000 series and NIST SP 800-55. The plan to use their existing ISMS as a basis for the establishment for measurements is what the existing standard and guideline, described in section 2.3, assume, so this could be a good starting point for the organization. They also plan to include reports from the supplier of their IT operations in the report they already present to the management. This will lead to a more holistic system for reporting. They wish to measure attributes that the management can understand, in order to increase the understanding for security actions. This is also something that is in compliance with the standard and guideline.

The interviewee mentioned that results should be presented to the management in a way that they can understand it and that this should help increase their knowledge regarding information security. This is in compliance with what is presented in chapter 2.

Organization B seems to have included relevant stakeholders in the process of developing their ISMS, and this could be a good basis for including them in the measurement processes as well. Both ISO/IEC 27004 and NIST SP 800-55 state that stakeholders should be included in the development of a measurement process.

Even though Organization B does not currently have a system for measuring information security they seem to be in the process of establishing a sound foundation for such a system. They satisfy several of the success factors from ISO/IEC 27004, that is listed in section 2.3.1, such as a, b and d. As they are in the process of establishing security controls and processes they could benefit from using implementation metrics, as defined in NIST SP 800-55.

5.3 Organization C

Organization C also uses the ISO/IEC 27000 family of standards. As with Organization B, they only use ISO/IEC 27001 and ISO/IEC 27002. They do perform a small amount of measurements, but they do not have a system for it. They perform penetration tests of parts of their systems, but they do not use any metrics related to this. They perform audits of their systems,

which could contain measurements, though it is somewhat unclear if there are any concrete quantitative metrics involved. The audits are used to increase knowledge and awareness related to information security, which complies with the goal of information security metrics.

This organization reports to a ministry that allocates money to them. They are required to report their information security in a certain way. Even though this does not mean that a form for management foundation for measurements is in place, it could be a start. It also shows that the ones that allocate money are concerned about information security. Such a foundation is one component in NIST SP 800-55's proposal for an information security measurement program. The management in the organization itself is not really involved in any measurement procedures.

Relevant stakeholders seem to be included in the audit processes, which is what theory discussed in section 2.3 recommends.

Organization C tries to compare results from measurements to previous results to discover any nonconformity. This is in compliance with proposed practice.

Incidents are reported, but not contained in any specific metrics. They have tools that go through their systems and check for old versions of applications. This data could have been used for a patch management metric, as explained in chapter 2, but as with the incidents, it is not.

Organization C seems to have some of the success factors described in section 2.3.1 in place. As they already use ISO/IEC 27001 and ISO/IEC 27002 they should have a solid base for the implementation of a process for measuring information security. The IT security manager's view on the importance of measurements supports this. The issue is that it is the management or a ministry that make decisions and that the initiative therefore must be originated there or at least supported by them. If they support this they will allocate money and a process for measurement of information security can be implemented.

5.4 Organization D

Organization D is a private organization that has used ISO/IEC 27001 and ISO/IEC 27002 as a basis for their security policy. They perform some

measurement, but do not have an overall system for it.

They generate reports that give information about the extent to which hosts have been updated with the latest patches. This could be used for a type of patch management metric, as described in 2.2. They repeat these measurements and compare the results to previous results, and it seems that this measurement is used in accordance with proposed practice. One aspect that may deviate from proposed practice is the reporting. The results are discussed, but not reported in a specific format. Even though it is not reported to the management in any specific ways, representatives from the management participate in discussions regarding results of some of the measurements.

Some results have been discussed with relevant stakeholders, such as audit results regarding access control. As mentioned, this is in compliance with both the standard and the guideline described in this report.

Their measurements are repeated and the results compared to previous results, which is what is recommended. They also use results to evaluate their current security actions and policies.

They wish to be able to correlate more logs and report data and a system for measuring information security would probably be beneficial for this organization.

5.5 Organization E

Organization E is a large government-owned organization that is highly dependent on IT and information security. They do some measuring and reporting but do not have an overall system for it. They measure incidents and virus infection in addition to receiving reports from their IT operations supplier about their IDS and firewall. In addition to measuring how many clients have been infected by virus they measure how many have been quarantined. These are numbers that could be used for a metric related to virus protection and handling of virus infections.

They have audits and tests related to security performed on their systems, but the results are not used in relation to any specific metrics.

The interviewee stated that one of their reasons for performing measurement is that they can use the results as a way of showing the management what

is going on. The results are used to increase the level of understanding of information security within the management. This may be an indication of some degree of management commitment, which is one of the success factors stated in ISO/IEC 27004. The management participates in discussions involving focus areas for the organization. These discussions could be a starting point for a foundation of management support of measurements, as described in NIST SP 800-55. Another success factor that they have in place is that they use results from measurements to identify what needs to be improved.

They use results from some observations as a basis for awareness activities for the employees. This is in accordance with one of the goals of metrics, but these observations cannot be classified as being information security metrics.

Organization E is still in the process of implementing the ISO/IEC 27000 series and it seems like they are in the process of getting a good base for an information security measurement system established. If they actually establish such a system is highly dependent on whether or not they will be required to do it.

5.6 Assessment of proposed metrics

This section assesses the applicability of the metrics described in section 2.2.

Risk assessment matrix, ALE, ROI and TCO are metrics that do not really evaluate the information security in an organization and are therefore not very applicable in an information security context. A risk assessment matrix could be used to assess risk, but this belongs to the area of risk assessment and not information security. The other three metrics involve estimates and it is difficult to get any useful results from them. This study did not reveal any use of the last three metrics.

The baseline defences coverage metric is applicable to all of the participating organizations. It is useful to examine if the implementation of basic defence tools (like antivirus and firewalls) covers all of the systems in an organization. It is however, important to be aware that the results do not give information of whether the tools themselves reach their goals or not. The patch latency metric is also applicable in practice and it gives indication of whether the

deployment of patches meets its goals. It does not give any indication of whether the patch itself reaches its goals or not. Practices similar to these metrics were revealed in the study, but they were not used in a systematic approach. These metrics could constitute a good starting point.

The password strength metric could be useful, but it might feel like a violation of privacy for the employees in an organization. The platform compliance scores metric is applicable in practice and is useful to examine if an organization's hardware configuration meet best practices. The goal of the vulnerability management metric is to ensure that all vulnerabilities are identified and mitigated, but it does not give any information about the identification of existing vulnerabilities and thus does not meet its goal. It is however, useful to examine if mitigation of identified vulnerabilities meets its goals. The access control metric give information about the robustness of remote access control. It is applicable for organizations that have systems that involve remote access. These metrics were not used in any of the organizations.

The contingency planning metrics is not tightly connected to information security, as it only gives information about the number of systems that have conducted contingency planning. The maintenance metric is not very applicable in an information security context. These two metrics are somewhat related to security in the sense that they indirectly indicate the availability of systems. The system and services acquisition metric is also of limited applicability as it only gives information about whether contracts include security requirements or not. It does not assess the actual systems and whether they are sufficiently secure.

For all metrics it is important to remember that results do not necessarily give information about how well an organization's systems are secured, but rather about to which extent implemented controls reach their goals.

Chapter 6

Conclusion and future work

All of the organizations studied seem to be performing some kind of measurements, but none of them seem to have a systematic approach. The measurements performed seemed to some extent to be random and the different measures were to a small degree related. Several of the interviewed organizations were in the process of introducing the ISO/IEC 27000 family of standards, where the main focus up until now had been on ISO/IEC 27001 and ISO/IEC 27002. None of them had looked at ISO/IEC 27004, which may be a natural place to continue the process. Several of the interviewees from government-owned organizations mentioned that if measurement of information security became a requirement, made by the government, this could help them get better at it, as they would have no choice. This is the reason why they introduced the ISO/IEC 27000 standards in the first place. They have a good point, because it can be hard to prove the usefulness of metrics. If it is required one does not have to provide arguments to get money allocated for it. On the other hand, metrics can be used to prove the effectiveness of information security processes and should therefore be attractive for the management in any case. Additionally they can be used to document if too many resources are spent on specific actions.

It was mainly the IT security managers that were the initiators for any measurement activities and that most of the organizations lacked the strong foundation of management support that NIST SP 800-55 mentions. The government-owned organizations used the ISO/IEC 27000 family of stan-

dards because of a requirement from governmental entities and thus one could say that measuring activities are to some extent required by management. ISO/IEC 27001 does specify that measurements should be performed. However in order for them to be able to focus more on measurements, they need to get specific requirements related to this, in order to be able to use resources on measurements. For most types of organizations the management needs to initiate or at least support the implementation of a system or program for measuring security if it is going to be done.

All of the interviewees thought that a standard for measurement of information security could be useful, as long as it is both general and specific enough. The standard should be general enough to be applicable for different types of organizations and specific enough to provide any real practical guidelines. In spite of this, none of the organizations had looked at any such standard, which may be an indication that they would like to measure security, but it is not prioritized. That may partly be because they lack the foundation of management support, and management commitment described in NIST SP 800-55 and ISO/IEC 27004.

Several of the organizations said that they were in an initial phase when it came to information security metrics, and some of them had plans related to it. This may indicate that measuring of information security will be more used in the near future, but one cannot really say based on these results. An interesting result was that a few of the interviewees mentioned that many people who work with information security in Norway know each other and that there are different arenas where they meet and thus get the chance to share experiences. This does not seem to be the general case in other countries. This type of network that exists in Norway can help organizations to get better at measuring security, if they use it to share their experiences.

There has been revealed a small amount of practices that are closely related to the existing metrics and standards discussed in this study. Systems or programs for the measurement of information security seem to be lacking in practice, at least in the organizations that participated in this study. Based on these results it it is apparent that information security metrics is still an immature area, at least in the interviewed organizations.

6.1 Future Work

Future work could include a comparison of how different types of organizations use information security metrics and if there are differences in which types of organizations that use it at all. Examples of comparisons are large vs. small and public vs. private. It would be interesting to see if there are any geographical differences when it comes to appliance of security metrics. This has been done in [19], but that was in 2005 and things may have changed. It would be interesting to compare results to that study, and any other existing similar studies, to see if things have changed or not. The focus that organizations have on information security is increasing and metrics for information security may become more used in the future. It would be interesting to conduct a similar study to this, or preferably in a larger scale, a few years from now and see what the situation is like then.

There exist standards and proposals to best-practices, but it could be useful to use these in combination with observed practices from organizations to derive a "best practice" for information security metrics. Even though it has been done before, some of them are somewhat vague and can be difficult to use. A new best-practice should include useful examples of concrete metrics, and more importantly, how to use them.

There exist several books, papers and standards that describe benefits of systematically measuring an organization's information security. It would be interesting to conduct a study that could actually show these benefits in practice. Such a "proof" could be a motivator for organizations to develop such a system.

Bibliography

[1] Shirley C. Payne. A Guide to Security Metrics. SANS Institute Information Security Reading Room, June 2006.

[2] George K. Campbell. How To Use Metrics. `http://www.csoonline.com/article/220980/how-to-use-metrics`, August 2006. CSO Magazine, visited 2012-10-12.

[3] ACSA and MITRE. *Information System Security Attribute Quantification or Ordering*. Workshop on Information Security System Scoring and Ranking, May 2001.

[4] Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo. Performance Measurement Guide for Information Security (NIST SP 800-55). Revision 1, National Institute of Standards and Technology, 2008.

[5] Lance Hayden. *IT Security Metrics: A Practical Framework For Measuring Security & Protecting Data*. McGraw-Hill Osborne Media, first edition, 2010.

[6] Andrew Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley Professional, first edition, 2007.

[7] ISO/IEC 27004:2009(E). Information technology - Security techniques - Information security management - Measurement - First edition. International Organization for Standardization, 2009.

[8] OECD. Guidance on Developing Safety Performance Indicators related to Chemical Accident Prevention, Preparedness and Response. *OECD Environment, Health and Safety Publications, Series on Chemical Accidents*, (18), 2008.

[9] W. Krag Brotby. *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement*. Auerbach Publications, first edition, 2009.

[10] Næringslivets Sikkerhetsråd. Mørketallsundersøkelsen - Informasjonssikkerhet og datakriminalitet, 2012. (In Norwegian).

[11] Reijo Savola. Towards a Security Metrics Taxonomy for the Information and Communication technology industry. In *International Conference on Software Engineering Advances, 2007. ICSEA 2007*, page 60, aug. 2007.

[12] Elizabeth B. Lennon. IT security metrics. ITL bulletin, August 2003. National Institute of Standards and Technology, 2003.

[13] William Stallings. *Cryptography and Network Security: Principles and Practice*, chapter 1. Prentice Hall, fifth edition, 2011.

[14] Scott Berinato. A Few Good Information Security Metrics. `http://www.csoonline.com/article/220462/a-few-good-information-security-metrics`, July 2005. CSO Magazine, visited 2012-10-12.

[15] Michael Fitzgerald. Security and Business: Financial Basis. `http://www.csoonline.com/article/394963/security-and-business-financial-basics`, June 2008. CSO Magazine, visited 2012-10-12.

[16] ISO/IEC 27002:2005(E). Information technology - Security techniques - Code of practice for information security management - First edition. International Organization for Standardization, 2005.

[17] ISO/IEC 27001:2005(E). Information technology - Security techniques - Information security management systems - Requirements - First edition. International Organization for Standardization, 2005.

[18] NIST. Recommended Security Controls for Federal Information Systems and Organizations (NIST SP 800-53). Revision 3, National Institute of Standards and Technology, 2009.

[19] Tone Hoddø Bakås. God praksis for måling av informasjonssikkerhetsnivå. Master's thesis, Høgskolen i Gjøvik, 2005. (In Norwegian).

[20] Gerd Lilledahl, Atle Wehn Hegnes, Tone Opdahl, Henrik Giæver, Finn Johansen, Hilde Rød-Larsen, and Tove Thagård. Kvalitativ metode. Forelesningsnotat, Sosiologi Hovedfag UiO, 2000. (In Norwegian).

[21] Michael D. Myers and Michael Newman. The qualitative interview in IS research: Examining the craft. *Information and Organization*, Volume 17, Issue 1:Pages 2- 26, 2007.

[22] Finansdepartementet. SMB-definisjoner. `http://www.regjeringen.no/nb/dep/fin/dok/nouer/1995/nou-1995-16/5/2/1.html?id=336716`. Visited 2012-10-29. (In Norwegian).

[23] Wikipedia. Information technology operations. `http://en.wikipedia.org/wiki/Information_technology_operations`. Vistited 2012-11-09.

[24] Atlassian. Jira. `http://www.atlassian.com/software/jira/overview`. Visited 2012-11-08.

[25] Tech-FAQ. ERP (Enterprise Resource Planning). `http://www.tech-faq.com/erp.html`. Vistited 2012-11-16.

[26] Maya Daneva and Roel Wieringa. Requirements engineering for cross-organizational ERP implementation undocumented assumptions and potential mismatches. In *Requirements Engineering, 2005. Proceedings. 13th IEEE International Conference on*, pages 63–72. IEEE, 2005.

[27] ISO/IEC 27005:2011(E). Information technology - Security techniques - Information security risk management - Second edition. International Organization for Standardization, 2011.

[28] Symantec. About Symantec, Business Overview. `http://www.symantec.com/about/profile/business.jsp`. Visited 2012-11-18.

[29] NSM NorCERT. About NorCERT. `https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/NorCERT/English/`. Visited 2012-11-18.

Appendix A - Information sheet and statement of consent

Forespørsel om å delta i intervju i forbindelse med en fordypnings-/masteroppgave

Jeg er masterstudent i kommunikasjonsteknologi med fordypning informasjonssikkerhet ved Norges Teknisk og Naturvitenskapelige Universitet (NTNU) og jeg holder på med fordypningsoppgaven min i forbindelse med mitt avsluttende år. Oppgaven kommer kanskje til å utvides til en masteroppgave neste semester. Temaet for oppgaven min er måling av sikkerhet og i tillegg til å gjennomføre en studie av eksisterernde måter å måle sikkerhet på, så ønsker jeg å finne ut av hvilke metoder bedrifter og organisasjoner faktisk bruker i praksis og på hvilken måte.

Jeg ønsker å foreta intevjuer ansikt-til-ansikt av personer fra ulike bedrifter for å finne ut av dette. Spørsmålene jeg ønsker å stille handler om hvilke metoder som brukes i tillegg til hvorfor og hvordan. Blant annet så lurer jeg på om dette brukes til å øke kunnskapen om informasjonssikkerhet i bedriften.

Jeg planlegger å bruke båndopptaker under intervjuene. Intervjuene kommer til å bli gjennomført i full fortrolighet og opptakene og eventuelle notater kommer til å bli oppbevart og behandlet konfidensielt på NTNU.

Intervjuene kommer til å bli foretatt av meg og noen deler kan bli diskutert med min veileder Maria B. Line, stipendiat ved NTNU og forsker ved SINTEF og professor Svein Johan Knapskog ved NTNU.

Resultatene fra intervjuene kommer til å bli en del av en rapport som leveres på NTNU. Ingen enkeltpersoner eller enkeltvirksomheter vil kunne identifiseres i denne rapporten. Ved prosjektets slutt, 01.07.2013, vil alle lydopptak bli slettet og øvrig datamateriale vil bli anonymisert.Det vil si at eventuelle direkte personidentifiserende opplysninger slettes og eventuelle indirekte personidentifiserenede opplysninger fjernes eller slettes.

Det er frivillig å være med og du har mulighet til å trekke deg når som helst underveis i prosjektet uten å måtte begrunne dette nærmere. Dersom du velger å trekke deg vil all samlet informasjon bli anonymisert og lydopptak vil slettes.

Dersom du har noen spørsmål kan er det bare å kontakte meg. Jeg håper du ønsker å delta.

Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelige datatjeneste (NSD).

Med vennlig hilsen
Marte Tårnes
martetar@stud.ntnu.no
Tlf: 98 47 40 67

Samtykkeerklæring:

Jeg har mottatt skriftlig informasjon og er villig til å delta i studien.

Dato/Sted: Navn: Signatur:

Appendix B - Interview guide

Intervjuguide

Information Security Metrics – good practice

Innledning

Hvem jeg er:

Masterstudent i kommunikasjonsteknologi med fordypning informasjonssikkerhet.

Kontekst:

Fordypningsprosjekt i forbindelse med avsluttende år på master. Prosjektet kan bli utvidet til en masteroppgave etter jul.

Forskningsspørsmål

a) Blir måling av sikkerhet gjort i praksis i virksomheter?
b) På hvilken måte forsøker de som måler sikkerhet å dra nytte av det?

Mål:

Målet er å finne ut om virksomheter måler sikkerhet på noen måte i det hele tatt og i så fall på hvilken måte og hvordan de bruker resultatene.

Formalia:

Tidsramme: ca en time

Jeg kommer til å bruke lydopptager.

Før intervjuet bes intervjuobjektene om å signere en samtykkeerklæring.

Spørsmål

Hovedparten av intervjuet er delt i to og er avhengig av om virksomheten måler sikkerhet eller ikke. Alle spørsmål, relatert til riktig kategori (om virksomheten måler eller ikke), kommer til å bli stilt med mindre de blir besvart som en del av andre spørsmål. Oppfølgingsspørsmål som dukker opp underveis i intervjuet kan bli stilt.

Innledende:

1. Hvor mange ansatte er dere i virksomheten?
2. Hva slags type organisasjon er dette/hva er kjernevirksomheten deres?
3. Hva er din rolle i virksomheten?

Måling av sikkerhet:

4. I hvilken grad er virksomheten avhengig av IT?
5. Hvordan er IT-driften deres organisert?
    a. Hvis det ikke nevnes, er deler av den satt ut/outsourced?

6. Gjøres det noen form for målinger eller rapporteringer i virksomheten som er relaterte til informasjonssikkerhet?
    a. Hvis nei:
        i. Vet dere for eksempel noe om hvor mange sikkerhetsrelaterte hendelser dere har?
            1. Hvis ja, gå til 6b
        ii. Teller dere antall timer nedetid på systemene deres?
            1. Hvis ja, gå til 6b
        iii. Hvis de har outsourcet deler av driften, rapporteres det noe fra leverandøren som viser at sikkerheten er god nok?
            1. Hvis ja, gå til 6b
            2. Hvis nei, hva gjør dere for å forsikre dere om at denne løsningen/disse løsningene er sikre nok/ hvordan kan dere vite at den er sikker nok hvis det ikke rapporteres noe?
        iv. Hva er grunnen til at dere ikke måler sikkerhet på noen måte?
            1. Har du noen tanker om kostnadene i forhold til gevinsten med å måle sikkerhet?
                a. Hvordan gjør dere prioritering av hva slags sikkerhetstiltak det er som skal utføres?
            2. Har dere vurdert det, men funnet ut at det er for vanskelig å få det til på en god måte?
            3. Hvem kunne ha vært involvert i en slik prosess? (mangler dere kunnskap/ferdigheter/ressurser?)
            4. Hva rapporteres til ledelsen når det gjelder sikkerhet?
            5. Er det noen andre grunner til at dere ikke måler sikkerhet?
        v. Hva slags data har dere som kunne ha vært brukt til å måle sikkerheten i virksomheten? (forskjellige typer loggdata for eksempel)
        vi. Bruker dere noe system for å rapportere hendelser (alle typer hendelser, som HMS)?
            1. Hvis ja, hvilket?
            2. Ser du noen måte dere kunne ha brukt dette systemet for rapportering av hendelser relatert til informasjonssikkerhet?
        vii. Hva slags nytteverdi ville dere hatt av å måle sikkerhet? (som bedre oversikt over sikkerheten i virksomheten, økt forståelse)
    b. Hvis ja:
        i. Kan du fortelle litt om hva slags målinger dere gjør?
            1. Er de kvalitative eller kvantitative (eller begge deler)?
            2. Kan du beskrive prosessen rundt det?
            3. Hva er det som måles (konkrete målepunkter)?
        ii. Hvorfor måler dere sikkerhet?
            1. Hva er målet med det?
            2. Hvilke(n) rolle(r) har de(n) som satte det i gang?
        iii. For hvilke deler av virksomheten gjøres det målinger?
        iv. Måler dere på noen måte om dere følger lover/forskrifter/standarder som omhandler informasjonssikkerhet?

1. Hvilke lover/forskrifter/standarder er det snakk om?
2. Kjenner dere til ISO/IEC 27004?
3. Er det også andre grunner til at dere gjør disse målingene?

v. Hvordan brukes resultatene av målingene dere gjør?
    1. Hvordan brukes målinger for å få en generelt bedre kunnskap om informasjonssikkerhet i virksomheten?
        a. Hvis dette ikke gjøres, hvorfor ikke?
            i. Hvilke muligheter for å gjøre dette kan dere se?
    2. På hvilken måte brukes resultatene for å forbedre sikkerheten i virksomheten?
    3. Brukes resultatene på noen andre måter?

vi. Hvilke roller har de som får presentert resultatene på noe vis?
    1. På hvilken måte brukes resultatene i arbeid for å øke bevisstheten rundt informasjonssikkerhet blant de ansatte?
    2. Hvordan presenteres de for ledelsen?
        a. Brukes de for å vise ledelsen nødvendighet av tiltak? (Hvis målinger gir dårlige resultat ser man at det bør gjøres noe)
    3. Hvilken nytte tror du de ansatte har av dette?
    4. (Brukes de kun blant de i virksomheten som jobber direkte med sikkerhet?)
    5. Presenteres resultatene på noen måte for kunder eller samarbeidspartnere?

vii. Hva sammenligner dere resultatene med?
    1. Tidligere resultater?
    2. Andre virksomheter?
    3. Forhåndssatte verdier man ønsker å oppnå?

viii. Hvor ofte gjennomgås resultatene?
    1. Er det faste rutiner på det eller blir det kun gjort hvis man merker eller mistenker at det har skjedd noe?

ix. Har du noen tanker om kostnadene i forhold til gevinsten med å måle sikkerhet?
    1. Føler dere at det er verdt det?
    2. Har dere noen gang vurdert å slutte med det, fordi dere ikke føler dere får nok igjen for det?

x. Hvordan synes du deres målesystem fungerer?
    1. Er det komplisert eller er det enkelt?
    2. Hva burde dere eventuelt gjort annerledes?

xi. Hvor stor ekstrabelastning/ekstraarbeid krever målingen dere gjør (inkludert eventuelle tiltak gjennomført i ettertid)?

xii. Bruker dere noe system for å rapportere hendelser (alle typer hendelser, som HMS)?
    1. Hvis ja, hvilket?
    2. Rapporterer dere også hendelser relatert til informasjonssikkerhet i dette systemet?
    3. Hva er nytteverdien av å gjøre det på denne måten?

7. Har du noen tanker om noe som kunne ha gjort det enklere for virksomheter å måle sikkerhet?
8. Hvilken nytte ser dere av en standardisering av måling?
    a. Tror du bruk av en standard ville ha gjort måling enklere?
    b. Hvilke utfordringer/ulemper med en standard for måling av sikkerhet kan du se for deg?