Measurement of Information Security - a cost benefit analysis of measurements at Norsk Pasientregister (NPR)

Sjur Hartveit

Masteroppgave
Master i informasjonssikkerhet
30 ECTS
Avdeling for informatikk og medieteknikk
Høgskolen i Gjøvik, 2011

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Measurement of Information Security - a cost benefit analysis of measurements at Norsk Pasientregister (NPR)

Sjur Hartveit

2011/01/23

Abstract

Measurement of information security seeks to improve the efficiency of the information security in an organization. Measurements can give advantages like:

- Enabling organizations to judge if the state of information security moves in the right direction over time
- Enabling benchmarking to see if they are performing better or worse than comparable actors
- Provide a basis for sound business decisions regarding information security
- Demonstrating compliance

However, when implementing security controls, it is important to know what can be expected in return on the investments. To justify adding another control like security measurements, the value gained should be larger than the costs of implementation.
Information security in Norwegian Health sector is regulated by a legal framework, but measurements are not compulsory. This thesis analyzes selected measurements through a case study in a Norwegian healthcare organization - the Norsk Pasient Register, NPR. The implementation in the case study is based on the recently published ISO/IEC 27004:2009 framework for information security measurement. A pilot on information security measurements was made in the case study and experiences gathered.

A survey is also presented regarding the perceptions of information security measurements and practices among Norwegian health trusts (HF's). Although guidelines for IS measurements have existed in Norwegian healthcare since 2004[1], the assumption is that there is little ongoing activity in this area.

The contributions of the master thesis is:

- more insight on validity and costeffectiveness of selected information security measurements.
- more knowledge on the perceptions and practices of information security measurements in Norwegian health trusts('Helseforetak' - HF's) and institutions.
- proposals for further research in this area

The study shows that measurements of information security is beneficial for an health organization. When it comes to perceptions and practices, more than 50 % states that they measure information security, but with limited knowledge on standards and guidelines. Measurements are seldom requested by management and some organizations lack formally stated goals for information security.

Sammendrag

Måling av informasjonssikkerhet søker å forbedre effekten av informasjonssikkerheten i en organisasjon. Slike målinger kan gi fordeler som:

- Mulighet for å bedømme om informasjonssikkerheten beveger seg i rett retning i en organisasjon.
- Muliggjør sammenlikning av status(benchmarking) for sammenliknbare aktører.
- Kan synliggjøre etterlevelse av relevante internt og eksternt regelverk (compliance).
- Utgjør et grunnlag for å treffe de rette beslutninger i organisasjonen.

Når det implementeres ytterligere sikkerhetskontroller, er det imidlertid viktig å vite hva som kan oppnås med denne investeringen. For å rettferdiggjøre innføringen av ytterligere kontroller, bør disse gi en større verdi enn kostnadene forbundet med å implementere de. Denne masteroppgaven analyserer utvalgte målinger i en norsk helseorganisasjon i form av et case-studie hos Norsk pasientregister (NPR). Implementasjonen av målinger i studiet baserer seg på en nylig publisert standard for måling av informasjonssikkerhet - ISO/IEC 27004:2009. En pilot på måling av informasjonssikkerhet er gjennomført i dette studiet og erfaringer innsamlet. Det er også gjennomført en spørreundersøkelse om hva slags oppfatninger/ gjeldene praksis som finnes rundt måling av informasjonssikkerhet i norske helseforetak (HF'er). Selv om det har eksistert anbefalinger for slike målinger i norsk helsevesen siden 2004 [1], så er antagelsen at det er lite aktivitet som pågår på dette området. Bidragene fra denne masteroppgaven er:

- Mer innsikt vedrørende gyldighet og kosteffektivitet på utvalgte målinger.
- Mer kunnskap om hvordan de ulike helseforetak/institusjoner oppfatter og praktiserer måling av informasjonssikkerhet.
- Forslag til videre forskning på dette området.

Studien viser at målinger av informasjonssikkerhet har nytte i en helseorganisasjon. Når det gjelder oppfatninger og praksis i helseforetak/institusjoner, så oppgir over halvparten at de måler informasjonssikkerhet, men har mindre kjennskap til målestandarder. Målinger er i liten grad etterspurt av ledelsen og noen organisasjoner har fortsatt ikke fastsatt formelle mål for informasjonssikkerhetsarbeidet.

Preface

To the author, this thesis marks the approaching end of a long journey of studying information security at Gjøvik University College (HiG).
First of all I would like to thank my family, especially my encouraging wife Mariann and my four kids for beeing patient with me in my years of studying.

Thanks goes to my advisor Einar Snekkenes for his support, advisories and critical comments during the project.

Thanks goes to my external advisor Arnstein Leonardsen at Norwegian Patient Registry but also to other employees of the registry who has helped me in the case study.

A special thanks goes to my opponent Jarle Kittilsen for reading my thesis and pinpointing areas for improvements. Thanks go to all the respondents in the survey who took their time to answer my questions, and especially the ones who provided me with names and access to the respondents.

Finally, thanks goes to my employer DIPS ASA for supporting my studies.

Bodø,

Sjur Hartveit, 2011/01/23

Contents

List of Figures

List of Tables

1 Introduction

'Security is like a chain; it's only as secure as the weakest link' - this statement by the famous cryptographer Bruce Schneier [3] is often put forward in discussions regarding information security. In an IT context, these 'links' can be thought of as the strengths and absences of vulnerabilities in various organizations, corporations, business processes, users, IT systems, components etc. Failure in any of these links can be a threat to the availability, integrity or confidentiality of information and affect business operations and delivery capabilities.
Personal information of individuals are gathered by these organizations and generally people have little control of how this information is taken care of. An example from the healthcare sector can be as follows: the sensitive information patients give to their primary care physician will not necessarily remain stored only on a computer hard drive in the physicians office. Previously, health information typically was stored in autonome systems, but in order to make the healthcare system more costeffective, systems are getting more interconnected[4]. An example of the latter is the Norwegian governmental 'Coordination Reform' for the health sector where one of the goals is coordination of efforts through the use of ICT.[5]
In order to secure information flowing between different entities, security activities and investments are done. Many of the activities undertaken are very similar in various organizations, whether it is to secure ATM transactions in a financial system or electronic medical records in a hospital. In order to secure information, organizations spend large resources on security measures like firewalls, anti-virus systems and risk analysis. However the business decisions for all this spending is often done on a relatively weak basis[6].
To remedy this situation, several frameworks and standards for *measuring* information security have been made, like the NIST SP 800-55 guide[7] and the ISO/IEC 27004[8] standard. Measurements can give long awaited feedback on the effectiveness of the various security controls, however little is known on the costs and validity on such measurements.

1.1 Topic

A goal of information security measurements is to increase the effectiveness of operational security in an organization[9]. Beside providing feedback on selected security controls for decision making[10], measurements can also provide benefits like increased accountability and demonstration of compliance[7]. Although these advantages seems obvious, measurements still does not seem to be focused in many organizations. If this is the case, what are the reasons for this and how can the value of some simple measurements be demonstrated to encourage measurements? This thesis discusses whether such measurements can be considered costeffective by studying an implementation in a health register - the Norwegian Patient Registry (NPR). It also investigates the perceptions and practices towards information security measurements in a selected area - the Norwegian specialist health care.

1.2 Keywords

Security measurements, security metrics, information security status

1.3 Problem description

The Norwegian health sector is under constant pressure to provide more efficient health services[5, p.13]. Information security in this sector is highly regulated through various laws and regulations[11], but information security *measurements* are not compulsory[12]. A survey performed in 2005 [13, p.29] suggests that few (29%) organizations in the public sector measure information security. If the cost of security measurements is larger than the benefits they provide, limited resources are probably used better elsewhere in the health sector where life and health are at stake. However, without feedback on security controls and measures, it is hard to tell whether information security in an organization improves or not.

1.4 Justification, motivation and benefits

Information security is vital to modern health care. Provididing health information of good quality and integrity in a timely matter (availability) is important to the life and health of the patient (patient security). Confidentiality of information is also important as *trust* is fundamental for the relation between patient and health personell. In a US pilot on a *distrust* indicator[14], more than 50 % was unsure, or disagreed to the statement 'My medical records are kept private'. Onabajo [15] states that 'inappropriate handling of medical records not only poses medical risk, but also social implications, such as discrimination'.
The number of reported security breaches of confidentiality in Norwegian health sector till now have been low, with relatively few medical records involved in each case[16]. In the US, security breaches are required by law to be reported and published[17] and they happen on a large scale like the recent disclosure of 4.2 million electronic medical records[18].

The Norwegian healthcare system currently has no legal requirements to *measure* information security and it is unknown to which degree Norwegian health institutions practices this. Without feedback from measurements, there is a possibility that organizations and institutions in this sector lacks the capability to ensure that information security is in accordance with their stated goals.

Knowing more about the value information security measurements brings to an organization will make it easier to get management support for instantiating a information security measurement program (ISMP).
This research will provide the following benefits:

- More knowledge on the value of implementing security measurements
- More knowledge on the practices and perceptions on information security measurement in Norwegian specialist health care.

Another outcome of this research is to identify suitable research questions to be studied further.

1.5 Research questions

Given the pressure to provide efficient health services, it is an assumption that activities like information security measurements might loose against more 'worthy causes'[1]. In this battle for resources, can information security measurements be considered to be cost-effective? Are measurements considered worth doing and are they actually performed? This thesis seeks more knowledge on the practices and perceptions towards information security measurements in Norwegian health institutions.
Based on the previous discussion, two research questions are formulated - the first one as follows:

Research question 1:
Are measurements of information security costeffective in an organization?

Sub reseach questions:

- *What are the efforts (costs) associated with providing the measurements?*
- *What is the validity of measurements?*

The second research question is formulated as follows:

Research question 2:
What are the perceptions and practices on information security measurements in Norwegian specialist health care?

[1] E.g. Improve cancer treatment by investing in a MRI scanner

2 Choice of Methods

This chapter first explains the choice of methods used to answer the research questions and then shows how these are used in the research strategy. When talking about a general strategy for solving a research problem, we are talking about the *research design*[19].

2.1 Research problem 1

Research problem 1 was formulated as follows:

Are measurements of information security costeffective in an organization?

In order to answer this question, several methods could have been used like:

- Survey
- Model construction
- Litterature study
- Case study

Surveys and case studies are methods for looking at the reality as it 'is'. Model construction is a more theoretical approach and is typically used when it is either impossible or impractical to create experimental conditions in which outcomes can be directly measured[20]. Since a case study is useful for 'learning more about a little known or poorly understood situation'[19, p.135], this qualitative method seemed suitable. The choice of the Norwegian Patient Registry as a case for further studying was also natural since the information security measurement topic originally was proposed by them.

The case study method was also chosen for the following sub reseach questions for the same reason:

- *What are the efforts (costs) associated with providing the measurements?*
- *What is the validity of measurements?*

2.2 Research problem 2

The second research question was formulated as follows:

What are the perceptions and practices on information security measurements in Norwegian specialist health care?

In order to answer this question, the quantitative survey method was chosen although multiple cases could also have been studied.

2.3 Research Strategy

Figure 1 shows how the research methods are used in this study. Due to time limitation for the thesis, it was necessary to perform the case study and survey in parallel.

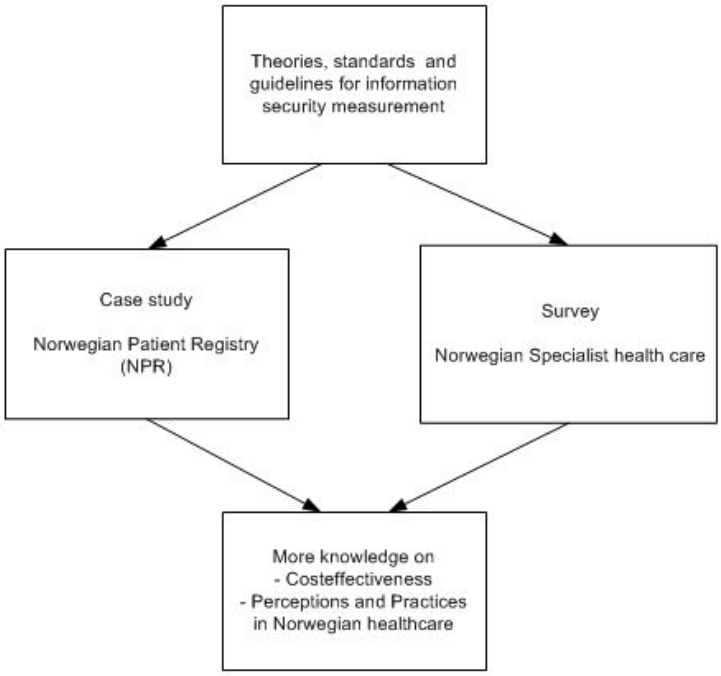

Figure 1: Research strategy

2.4 Case study

If the introduction of security metrics in an organization has a positive effect, the chances are good that this also will have positive effects on other organizations as well. It is however difficult

to generalize from this case into the whole population. If a number of positive case studies show that the measurement of information security has a positive effect, the chances increases that measuring is worthwhile.
In more 'pure' case studies, the researcher should not be directly involved, but the researcher has here taken a more active role in order to implement measurements. The answers to the research question will lie in the experiences drawn from this study.
According to [10, p. 022], the measurements selected should be consistently measured and cheap to gather. They should also be expressed as a number or percentage suitable unit(s). Much of the same ideas are expressed in ISO27004 [8, p. 015], which also states that measurementss that potentially could satisfy the selected information need should be selected. The standard also lists a number of example criterias for measurement selections like easy and cheap to gather, available human resources and tools for gathering and managing the data and costs.
In [1, p. 10] two basic approaches for measurements selections are stated, the *top-down approach* and the *bottom-up approach*. In the top-down approach, the goal for the measurement is stated first, then the various indicators are selected in order to achieve the goal. In the bottom-up approach, various possible measurements are selected first, then they are evaluated against the main objective for the measurements.
The ISO/IEC 27004 standard will be used as a guidance in the case study.

2.5 Survey

To further put the results from the NPR case study in a context, it was decided to conduct a survey in the form of interviews of selected persons in the Norwegian regional health trusts (HF's).Surveys are commonly used in research regarding information security, but according to [6], there are a number of weaknesses with such surveys. These can be summarized as follows:

- Biased questions
- Finding (the right) respondents
- Organizations are in general unwilling to talk about security failures
- Self selection (can be avoided through active selection of interview subjects)
- 'Valence or reverse' valence effect[1]

Although plagued with weaknesses as stated above, the survey should provide more knowledge on the perceptions and practices of security measurements, and the design of the survey will attempt to address these issues.

[1] People's tendency to overestimate the likelihood of good things happening rather than bad things. Security professionals 'in the trenches' will likely have the opposite tendency of thinking that things are worse than they are

3 Related Work

The following chapter contains an introduction to information security measurements with related work. First an explanation of information security measurements is presented along with some of its supposed benefits. Measurement theory is accounted for along with some definitions and criticism of information security measurements.

3.1 Introduction to Information Security Measurement

The synonym 'Security Metrics' is perhaps a more widely used term for measurements[21, p.6], but this thesis will mainly stick to the terms and definitions of the measurement standard ISO/IEC 27004:2009[8] which builds on the terminology from ISO/IEC 15939:2007[22].

'You can't manage what you can't measure' is a quote from Robert S. Kaplan[23], one of the creators of the *balanced scorecard* which is commonly used in business management. As a misquote it is commonly attributed to W. Edwards Deming. He, on the contrary, stated that that management should not be 'Running a company on visible figures alone' as many important factors are 'unknown and unknowable'[24][1].
It is difficult to model reality by measuring every aspect of information security, and it is imperativ to select the measurements that matter (Key Performance Indicators - KPI). Savola states that the *granularity* of measurements is also important, see figure2 [2]. Jaquith[10, p.20], gives

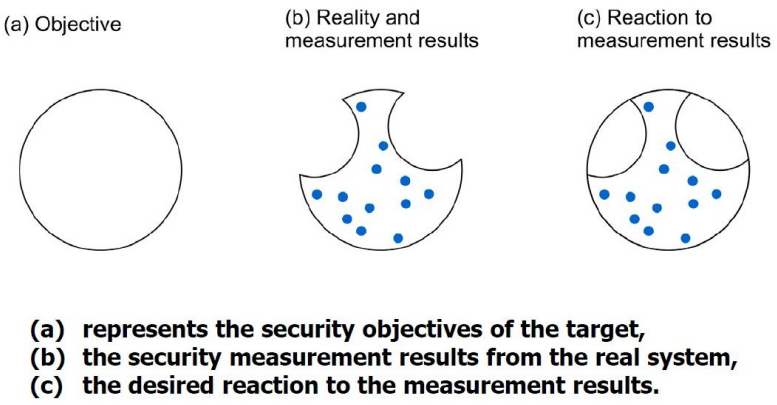

Figure 2: Granularity of security measurements (metrics)[2]

examples indicators that have proven successful in other disciplines, like the 'Inventory turns' used in warehousing (total cost of goods sold annually divided by average inventory value for that period).

[1] Disease number 5 of the 'Seven Deadly Diseases of Western Management'

A frequently referenced book in the measurement litterature is A. Jaquith - *'Security Metrics - Replacing Fear, Uncertainty and Doubt'*. Here, the primary goal of security measurements is to 'quantify data to facilitate insight'[10, p.21]. This insight then should be used to support decision-making regarding information security.

According to ISO/IEC 27004 standard [8, p.4], the goals of Information Security Measurements includes the following (abbreviated):

- evaluate the effectiveness of the implemented controls or group of controls
- evaluate effectiveness of an Information Security Management System (ISMS)
- verify if security requirements have been met
- facilitate performance improvement of an organization's overall business risk
- support decision making and justify improvements of an ISMS

The data gathered from measurements can both be quantitative or qualitative. Many books on security measurements (or the more common term 'security metrics') starts with citing Lord Kelvin's statement that 'When you cannot express it in numbers, your knowledge is of a meager or unsatisfactory kind'[2]. Jaquith [10, p.22] supports the view that quantitative data should be used in measurements, while others like Hayden [21, p.63] also supports the use of qualitative data. Data is then turned into information and further 'refined' as knowledge and ultimate wisdom (DIKW hierarchy).

3.2 Measurement theory

Information security 'metrics' has been a common term for the measurement of information security, however this term is ambigious[25][21]and the trend is towards using the term 'measurement' as used in the ISO/IEC 27004:2009 standard [8]. Some of the most important key terms in the standard are defined as follows:

- Measurement - process of obtaining information about the effectiveness of ISMS and controls using a measurement method, a measuement function, an analytical method, and decison criteria.
- Measure - Variable to which a value is assigned as the result of measurement.
- Attribute - Property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means.
- Base measure - Measure defined in terms of an attribute and the method for quantifying it
- Derived Measure - Measure defined as a function of two or more values of base measures.
- Indicator - Measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to information needs.
- Analytical model - algorithm or calculation combining one or more base and/or derived mea-

[2]This citing (or misciting) is a common tradition for litterature in this area

sures with associated decision criteria

From these definitions, the process of measuring can be described as measuring *attributes* by using one of more *base measures*, then combining them into *derived measures*. An analytical model is then used for making decisons and aggregating the measures into an *indicator* (the highest level).
A simplified visualisation of this process could be to think of an object (car) with several attributes (oil pressure, engine temperature) which are measured through base measurements and combined into a derived measure (engine status). By using an analytical model (temperature > 90C) the evaluation (of the temperature) is provided to an indicator (warning lamp in dashboard) for decision making (stop the car!).

3.3 Criticism

Information security measurements has also been subject to criticism. Bellovin[26] has discovered that 'defining metrics is hard, if not infeasible, because an attacker's effort is linear, and exponential security is needed'. McHugh [27] is skeptical of the side effects of such simplification and the lack of scientific proof. Burris & King[28] states that luck also plays a major role in security especially in the weakest links of information security solutions.
Although the citicism makes important points, the alternative of not measuring does not appear as a tempting alternative. Security measurements, although flawed and with little precision, might give advantages like incremental improvements in information security leading to an increased overall security level.

3.4 Security Measurement Standards and Frameworks

This section contains a short description of measurement standards or related standards.

3.4.1 NIST SP800-55

The National Institute of Standards and Technology Special Publication (NIST SP800-55) provides guidance on identifying information security measurements for security controls, policies, and procedures. In its current version *NIST SP 800-55 Revision 1, Performance Guide for Information Security*[7], it provides help for decision making and investments in security protection resources. It also provides guidance for identication and evaluation of nonproductive controls. The first version was published in 2003 as *NIST SP 800-55, Security Metrics Guide for Information Technology Systems*[29]

3.4.2 ISO/IEC 27004

The *ISO/IEC 27004, Information Technology - Security Techniques - Information Security Management - Measurement*[8]is a recent standard published in 2009. This standard is influenced by several national standards like the NIST SP 800-55 and complements the security management standard *ISO/IEC: 27001:2005 Information technology - Security techniques - Information security management systems - Requirements* [30]. According to this standard, the effectiveness of security controls must be measured. The figure 3 shows how the ISO/IEC 27004 measurement activities fit into the Plan-Do-Check-Act (PDCA), an iterative four-step management method.

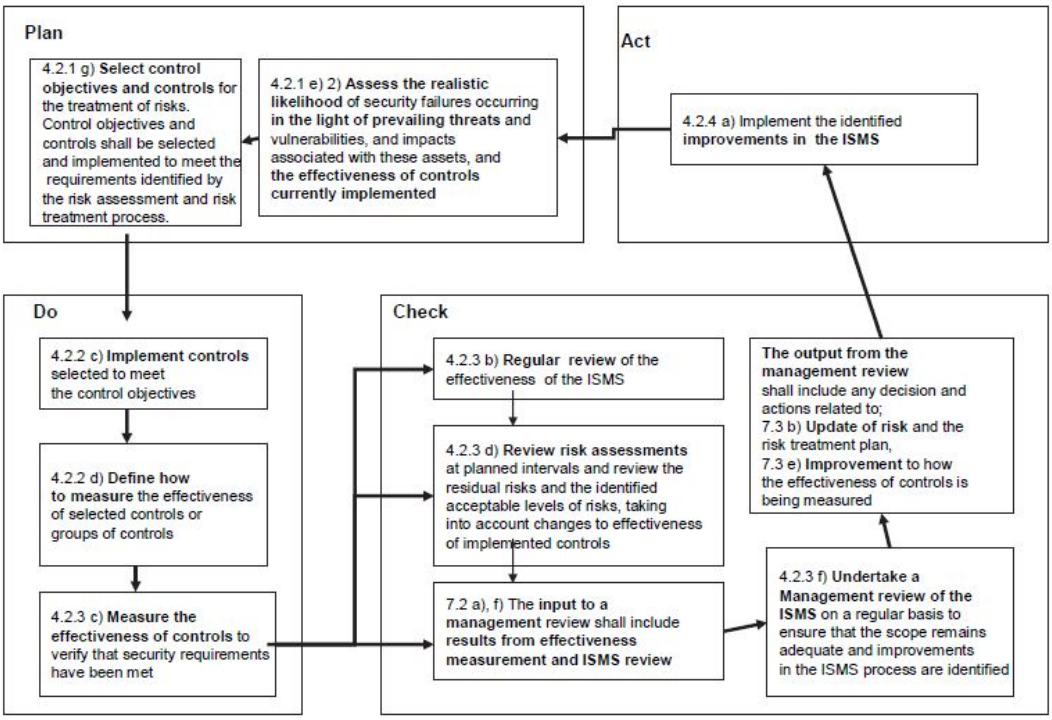

Figure 3: ISO 27001 PDCA with measurement activities
[8]

3.4.3 ISO/IEC 15408

The ISO/IEC 15408[31] standard also known as the 'Common Criteria' is a framework where the security, functional and assurance requirements of computer software can be evaluated against specific targets. As such, it *measures* the assurance level of security.

3.4.4 FIPS 140-2

The *Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules*[32] has a corresponding verification programme (CMVP) that can measure the strength in cryptographic modules.

3.4.5 KITH R08-04

Although not a standard, these guidelines have been specially tailored for use in Norwegian healthcare. It is inspired by the NIST SP 800-55 but has not been implemented as a part of the 'Code of conduct for information security in the health sector'[12]. The KITH guidelines describes what indicators for information security measurement are, how they can be implemented in a system, description for indicators and a list of suggested indicators.

3.4.6 COBIT

The "Control Objectives for Information and related Technology" [33]is a best practices framework from ISACA for linking business goals to IT goals. It contains measurement and maturity models to measure achievements in several areas.

3.4.7 ISF Survey

Information Security Forum (ISF) [34] provides tools for benchmarking (measuring). The tools are the ISF Benchmark (former Security Status Survey) and Fundamental Information Risk Management (FIRM).

3.5 Economics of measurements

Economic considerations of information security in general (or the lack of such) has been adressed in several publications since the early '70's. In [35], cost benefit consideration of protection is discussed, among others the cost of computational overhead at performing Vigenère ciphering on a CDC 6600. Their conclusion is still valid and concludes that

> The design of cost-effective data security safeguards for personal information databank systems[3] requires a careful balancing of the value of protected information against the protection costs. In particular, it is important to consider not only the value of personal information to the subjects, but also to the potential intruders, i.e., the protection investments should be made on a rational basis.

The *value of protected information* is not always easy to assess, especially not in a health context. Some proposed methods for analysis are discussed in the following.

[3]The term databank implies a centralized collection of data to which a number of users have access.

3.5.1 Cost-benefit analysis

A *cost benefit analysis*(CBA)[4] simply compares the cost of an activity to the benefits of that activity.[36, p.20] A cost-benefit analysis of information security measurements can be difficult to perform. The costs of information security measurements can usually be established, but the benefits can be very difficult to state in monetary values with a reasonable degree of accuracy. Often the benefits are derived from cost savings (aka. 'cost avoidance').

Information security measurements are associated with costs, both direct costs related to the measurements themselves but also indirect costs may occur e.g. loss of productivity when generating reports on access control rights in a database is causing slow responses in a production application. Costs of information security measurements can be related to the various activities:

- The initial process of choosing the right measurements
- Initiation of measurements
- Operations of measurements
- Presentation of measurements
- Disposal of measurements

3.5.2 Annual Loss Expectancy

According to [36, p.75], the Annual Loss Expectancy (ALE) first appeared in the now withdrawn NIST guideline Federal Information Processing Standard (FIPS) 65 *'Guideline for Automatic Data Process Risk Analysis'*. The ALE is widely known and used in information security circles and can be defined the following way:

$\mathrm{ALE} = \mathrm{ARO} \times \mathrm{SLE}$

where ARO equals the *Annualized Rate of Occurence* and SLE equals the *Single Loss Expectancy*[21, p.15] The ALE is widely criticized for unrealistic assessment of the loss expectations caused by unknown probabilities (lack of reliable historical data and costs from previous incidents)[21][10]. Modeling outliers and sensitivity to small changes in assumptions are also problems[10]

3.5.3 Return on (Security) Investment)

Return on Investment (ROI) and the similar Return on Security Investment (ROSI) has been borrowed from the business world. The ROI is calculated by subtracting the investment from an expected loss eg. spending NOK 100.000 in order to avoid a loss of NOK 1.000.000 from a security incident will gain a NOK 900.000 return on the investment (ROI). This method is highly criticized[37, p.119],[21, p.17]. The problem with using this method is much the same as with ALE, it is hard to estimate both the *probability* (main reason) but also the *impact* of a security related event.

3.5.4 Net Present Value

Net Present Value improves the concept of ROI/ALE by intruducing discounting of the cashflow. In [36] it is defined as a 'method for selecting capital investments based on the difference between the present value of the future cash inflows by a project and the projects initial cost. The

[4]The term Benefit-Cost Analysis, BCA is also in common use

'2010 / 2011 CSI Computer Crime and Security Survey' [38] shows that the NPV is gaining acceptance from information security community on the expense of ALE and RO(S)I.

3.5.5 Internal Revenue Rate

Internal Revenue Rate (IRR) is described in [36] as 'The discount rate that equates the present value of future cash inflows from a project to the project's initial cost. The IRR iso also used as a method for selecting capital investment'.

3.5.6 Cost-effectiveness

The concept of cost-effectiveness is well known in medicine and frequently used for comparison of various treatments, eg. spend money on anti-viral medicines compared to the alternative of beeing confined to bed at home, with both alternatives having different costs and probabilities. Muennig [39] states that cost-effectiveness is an effective way of comparing the costs of alternative treatments when the benefit (good health) cannot be stated in montary terms. In medicine they have invented the QALY (Quality Adjusted Life Year) which avoids the dilemma of assigning montary values to health, but instead estimates how much it cost to by a year of lifetime in 'perfect'. Similar thinking might be applied to information security.

4 NPR in the Norwegian health system

This chapter contains an introduction to the organization of the Norwegian specialist health care system and the role of NPR is explained within this context. The NPR contains sensitive personal information and the legal framework for protecting the information is given account of. There are several stakeholders with an interest in security measurements at NPR and these are also discussed.

4.1 Norwegian health care

The Norwegian health care system[40] is built around the principle that all members of society have universal coverage. This system has mechanisms for health financing and service provisioning and is generally referred to as *Universal health care*. Health care facilities are largely operated by the public sector in contrast to e.g. United States where this is operated by the private sector and based on private and public insurance programs.

4.2 Public sector and its national health registries

The Norwegian health management is performed at three different levels [40, p.14]:

- National level
- Provincial level
- Local level

The Ministry of Health and Care Services (HoD - Helse og Omsorgsdepartementet) operates at the national level and formulates and implements the health policy. The ministry has several subordinate agencies like the Norwegian Directorate of Health (Helsedirektoratet) which is responsible for providing ordinances, national guidelines and campaigns. The directorate also advices the ministry on legislation and health policy and manages grants for service projects and research. NPR is one of the (at the time of writing) following 10 central health registers in Norway:

1. Medical birth registry (Medisinsk fødselsregister)
2. Institute of population based cancer research (Kreftregisteret)
3. National Immunisation Registry (System for vaksinasjonskontroll - SYSVAK)
4. Defence Health Registry (Forsvarets Helseregister)
5. Norwegian Patient Registry (Norsk Pasientregister - NPR)- an entity in the Directorate of Health
6. Norwegian Surveillance System for Communicable Diseases (Meldingssystem for smittsomme sykdommer - MSIS)

7. Tubercolosis Registry (Det sentrale Tuberkolose Registeret)
8. National Prescription database (Nasjonal database for elektroniske resepter)
9. National Registry of Cardiovascular diseases (Nasjonalt register over hjerte- og karlidelser) - this register is currently beeing implemented.
10. Cause of Death Register (Dødsårsaksregisteret)

Most of these registers are operated by NIPH - Norwegian Institute of Public Health (FHI - Folkehelseinstituttet) which is the main source of medical information and advice. A new national registry for care summary records (Kjernejournal) is in the planning phase and will after its implementation contain medication information, critical medical information and contacts with specialist health care. The registers get their information mainly from general (somatic) and psychiatric hospitals and primary health services. The registers processes the information according to their own purposes and provides information for public administration, financing, statistics and public/private medical research. The registers are legally regulated by the Personal Health Data Filing System Act (Helseregisterloven - 'Health Registry Act') [41] and most have their own special regulations. The regulations states that the registers (mostly) are allowed to do allignment of data with each other. The figure 4 shows the registers with information flow pathways. The interconnections at the register layer forms an almost fully connected graph[1].

4.3 Specialist health care

Norwegian specialist health care services include general hospitals (somatic) and hospitals for psychiatric/psychological disorders. The specialist health care also include various centers and facilities like centers for training and rehabilitation, institutions for drug addicts etc.

These specialist services are not directly organized at the provincial layer, but organized in four 'health enterprises' called Regional Health Authorities (RHF), one for each part of Norway. See figure 5 for an overview. The various health trusts are organized below their respective RHF's and may well consist of several hospitals.[2]. All the health trusts are required to regularily report on their activity data, waiting lists for treatment and national quality indicators to NPR.

4.4 Primary health care

The Norwegian local authorities (430 municipalities) are responsible for the primary health care services. The municipalities are responsible for providing care and treatment of all persons within its geographic boundaries. According to [40], the services include general practices, pregnancy and antenatal care, health clinics for mother and child, school clinics, mental health care, nursing homes, rehabilitation, physiotherapy, communicable disease control, preventive medicine, environmental health and health promotion. Some of the entities providing these services are also required to report their activities to NPR regularily .

[1] A primer on graph theory in an ICT context is given in [42]
[2] E.g. the general hospital at Gjøvik is a part of 'Sykehuset Innlandet HF' which is owned by Helse Sør-Øst RHF

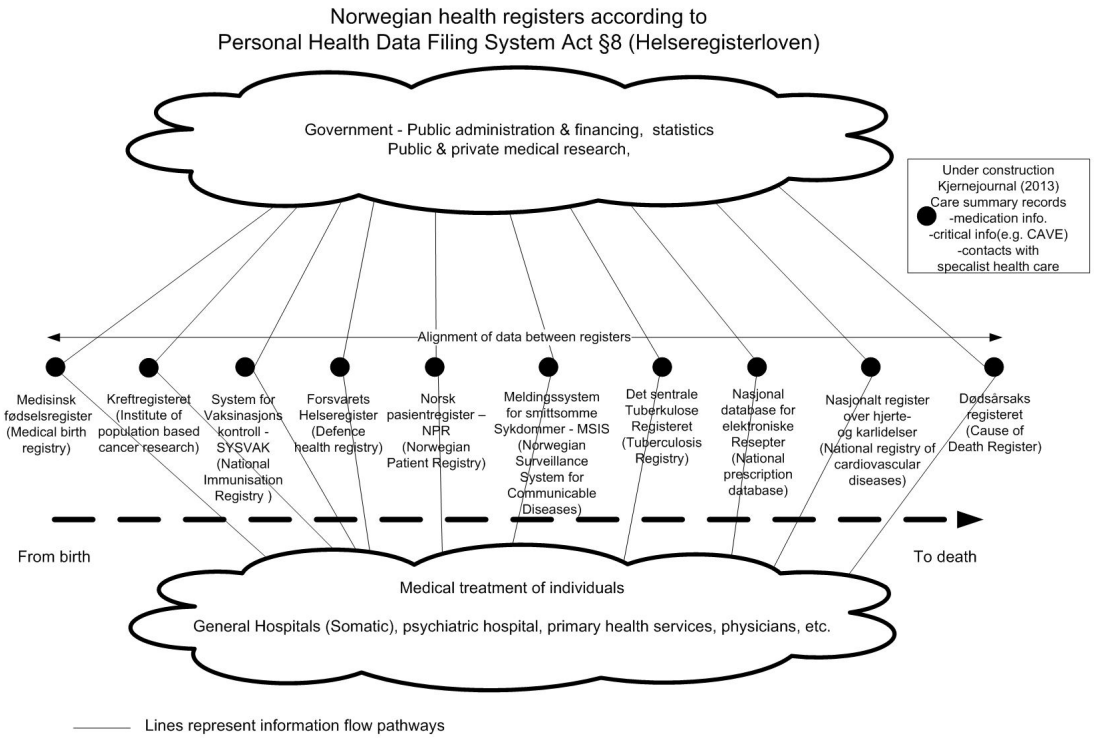

Figure 4: The central health registers in Norway with information flow pathways

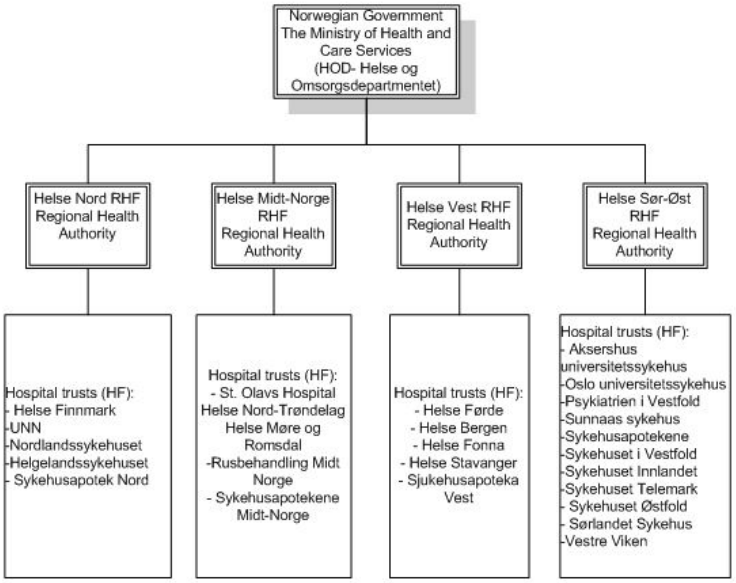

Figure 5: Norwegian Specialist Health Care - Organization chart

4.5 About NPR

The Norwegian Patient Registry (NPR) is a department in the Health Economics and Financing Division of the Norwegian Directorate of Health. The registry was established as a deidentified registry in 1997 by the SINTEF Group, an independant research organisation in Norway. NPR was originally a part of the SINTEF Health Services Research funded by the Norwegian government.

The main purpose of the register was initially to provide data for the administration and public funding of Norwegian specialist health care. The medical research community had used the register for some time, but were restricted by the data subjects beeing deidentified.

The decision to change the NPR from a deidentified register, to a register containing fully identified data subjects came in 2007 and was controversial. The Data Inspectorate[3], was for data privacy reasons negative to the register beeing able to identify data subjects, and suggested the use of pseudonyms instead. The view of using pseudonyms in health registers is also promoted in sources like [43]. But, partly due to medical research arguments promoted by agencies like The Norwegian Institute of Public Health [44], the register finally was required to register peoples identities. At the same time, the NPR unit was transferred to the Directorate. Today the registry serves these purposes:

- to provide data and statistics for planning, evaluation and financing for publicly funded specialist health care, including needed data for the activity-based financing

[3]Independent administrative body under the The Ministry of Government Administration and Reform

- contribute to medical and public health research
- provide basis for the establishment of and to ensure quality in other disease or quality registries
- contribute to knowledge for the (proactive) prevention of accidents and injuries

The volume of health information that the register posseses and the role as a major 'hub' in the Norwegian health care information flow, makes NPR a very interesting case.

4.6 Data in the NPR

Public and private[4] health institutions in Norway are required by health regulations to regularily report their activities to NPR. The requirements are stated in the NPR regulation[45]. Due to the sensitivity of personal health information, the data to be reported is split in two separate parts - one containing the required data coupled to a hospital specific personal ID number (PID), the other containing the Norwegian birth number ('SSN') and the PID. The last part makes it possible to fully identify the data subject and this information is stored encrypted in the register. As soon as the encryption has been done, the cleartext version of the PID and the birth number is deleted. The data to be reported by health institutions consists of the following:

- Information about the data subject (Birth number, social security number or similar, municipality)
- Administrative information
- Medical information (e.g. area, conditions and diagnosis (ICD10), surgical procedures (NCSP), medical procedures (NCMP))
- Social information (habitat, family relations etc.)
- Information about injury/damage from acute reception of patients in hospitals and selected municipal general emergency practices

Information containing medical information is regarded as sensitive personal information in the Personal Data Act[46] and NPR will over time contain a large[5] part of all health related information for the entire Norwegian population[6].
The weighted directed graph in figure 6 illustrates the flow of health information from various sources towards destinations (the disclosures) from NPR.

4.7 NPR and information security

The section describes some aspects of information security at NPR. The legal framework is presented along with risk acceptance criterias from the information security policy. The status of the ISMS is also discussed.

[4] Reporting from private institutions required for activities financed by the public health care
[5] As the register contains mostly structured information, the unstructured details in a patient's journal (plain text) is not registered
[6] Including special cases like VIP's

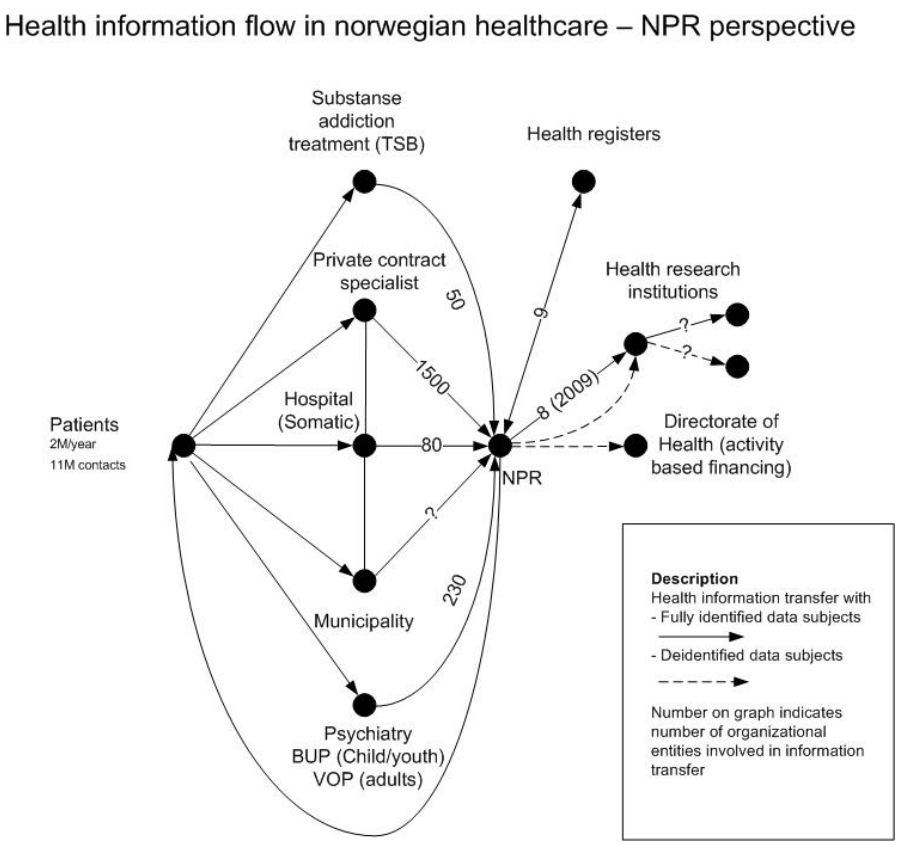

Figure 6: Health information flow in Norwegian healthcare - from a NPR perspective

4.7.1 Legal aspects

The need for information security when dealing with electronic health information is obvious and is stated in Norwegian acts with their respective regulations - one is specially tailored for NPR (This regulation is discussed further below). In general, Norwegian health informatics is mainly regulated by the following acts[11, p.54]:

- The Health Personnel Act (Helsepersonelloven)
- Patients' Rights Act (Pasientrettighetsloven)
- Specialist Health Care Act (Spesialisthelsetjenesteloven)
- Mental Health Care Act (Psykisk helsevernloven)
- Act relating to the municipal health services (Kommunehelsetjenesteloven)
- Regulation relating to Electronic Medical Records (Journalforskriften)
- Personal Data Act (Personopplysningsloven)
- Personal Health Data Filing System Act (Helseregisterloven)
- Archive Act with regulations (Arkivloven med forskrifter)
- Working Environment Act (Arbeidsmiljøloven)

There are also laws governing medical research like the Act on medical and health research (Health Research Act). To make it easier to be compliant with all these laws and regulations, a 'Code of Conduct for information security in the healthcare, care, and social services sector'[12] has been published by the Norwegian Directorate of Health. Beeing compliant with 'The Code' will automatically lead to compliance with most laws regulating information security in the healthcare sector.
But there are special regulations as well. Recognizing the large consentration of sensitive information and the importance of information security, lawmakers regulated information security as a part of a special regulation for the register ('NPR forskriften')[45][7]. Section 4-2 in the regulation is devoted to information security and states the following[8]:

- *The Directorate and Norsk pasientregister shall through planned and systematic measures, ensure good information security with regards to confidentiality, integrity, quality and availability for the processing of health information following the regulation.*
- *The security measures shall contain measures that cannot be influenced or circumvented by employees at Norsk pasientregister, and not be limited to expected acts by individuals. Systems shall be established for logging electronic traces for all access to the register*[9]
- *Where the processing of health information is done in whole or partly by electronic means, the conditions on information security given in the Personal Data Regulations [47] §2-1 to §2-16 apply*

[7] The regulation belongs to the The Personal Health Data Filing System Act
[8] Authors own translation
[9] Interestingly, review of logging is not stated in the regulation itself or its comments

As a 'planned and systematic measure', measurements of information security can help the register beeing compliant with the regulation.
Information security is also regulated through section 4-3 giving requirements on encryption of personal identification numbers.This section states that identifiers which can be directly linked to a person, typically beeing the Norwegian birth number (unique ID number like the US Social Security Number), shall be stored encrypted. Only persons working in the NPR organizational unit or working under instructions from NPR are allowed access to the register on a need-to-know basis. Only specially authorized persons are allowed to access unencrypted data in the register.

4.7.2 Policy for information security at NPR

NPR is governed by the information security policy in the Norwegian Directorate of Health which states that the availablility of information systems should be high (non-planned disruptions in dataprocessing systems should not exceed more than 2 incidens pr. half-year, each not lasting longer than a period of 1 hour), and that personal information always shall be given to the right person and not compromized (zero toleranse on confidentiality and integrity breaches). Consequences of not beeing compliant to the policy is not explicitly stated in the policy. The ISMS at NPR is currently undertaking a major revision which makes it difficult to attach the ISMP directly to it. The new ISMS will be defined according to the Code of conduct for information security in the health and social sector [12].

4.8 Stakeholder analysis

Stakeholders are very important in the ISO/IEC 27004 standard and this word is used more than 50 times throughout the document. In the Introduction section, it is stated that

> The Information Security Measurement Programme will encourage an organization to provide reliable information to relevant stakeholders concerning its information security risks and the status of the implemented ISMS to manage these risks

.

In the project management dicipline, a common definition of stakeholders are as follows[48]

> Individuals and organizations who are actively involved in the project, or whose interests may be positively or negatively affected as a result of project execution or successful project completion.

A similar definition of stakeholders should have been made in the ISO standard e.g 'those who may be positively or negatively affected, directly or indirectly, by the measurement processes or their results'.
Althought the 'stakeholder' term is not explicitely defined in the 'Terms and Definitions' chapter of the standard, examples of stakeholders are given in chapter 7.5.8[10]:

- Client for the measurement
- Reviewer for measurement

[10]The same stakeholder terms are used in the Annex B containing Measurement construct examples

- Information owner
- Information collector
- Information communicator.

4.8.1 Stakeholders for information security measurement at NPR

Two kinds of stakeholders are considered here - internal stakeholders are individuals working inside the organization at NPR or the Directorate of Health (Helsedirektoratet). External stakeholders are those outside of the organization. From conversations with NPR, the following internal and external stakeholders were identified[11]:

External stakeholders:

- Norwegian Board of Health Supervision (Helsetilsynet)
- The Data Inspectorate (Datatilsynet)
- Vendors[12]
- Data subjects (registrerte)
- Data providers(rapporteringspliktige)

Internal stakeholders:

- Norwegian Directorate of Health (Helsedirektoratet)
- Management
- Information Security Coordinator
- Section leaders
- System owners
- Team leaders
- Employees

[11] Counter stakeholders were not identified in this process

[12] Vendors can also be seen as an internal stakeholder when working as a data processor under the instruction of the data controller.

5 NPR - Internal survey on measurements

This chapter contains the design and results from an internal survey on information security measurements at the Norsk Pasientregister, NPR. The purpose of the internal survey was to gather information needed for later selection of measurements considered important for the various stakeholders at NPR.

5.1 Presentation of Information security measurement and ISO/IEC 27004

Initially two meetings were held at NPR to introduce the concept of security measurement and the work to be done in this master thesis. One meeting was held for the senior management/staff and one meeting for the various team leaders.

5.2 Initial scope

According to ISO/IEC 27004 subclause 7.2:

> Depending on an organization's capabilities and resources, the initial scope of an organization's measurement activities will be limited to such elements as specific controls, information assets protected by specific controls, specific activities for information security that are given highest priority by management.

In order to know which areas that was prioritized and should be considered for measurements, stakeholders like management and key persons in the register were challenged.

5.3 Information needs

Various stakeholders have different information needs and the following internal stakeholders was considered:

- The Norwegian Directorate of Health (Helsedirektoratet)
- Information Security Coordinator at NPR.
- Management
- Section leaders
- Team leaders
- System owners

Two persons from senior management at Helsedirektoratet was asked which measurements of information security they considered as most relevant and should be watched carefully. The executive officer of the Health Economics and Financing Division responded with a suggestion on the following areas:

- Access to information should be on a 'need to know' principle.
- Technical measures against external intruders eg. number of intrusion attempts
- Employee security awareness, especially regarding handling of removable media (eg. paper, laptops, cd's etc.)

The security leader at Helsedirektoratet suggested possible areas like:

- violation of policy regarding acceptable risk
- violation of security policy by users
- discrepancy and discrepancy reporting
- violation of dataprocessing agreement, system availability, Service Level Agreement (SLA), error situations and causes of such
- error conditions in logging systems
- security audits undertaken
- incidents with consequences for NPR and patients (data subjects in the register).

In order to gather further information about the information needs from management, section leaders and team leaders at NPR itself, a small internal survey was carried out inm the organization. The goal of this survey was to find out roughly which area (if any) the various respondents considered as interesting candidates for measurements.

5.4 Design of internal survey at NPR regarding Information Needs

The design of this survey is discussed in the following:

5.4.1 Type of survey

The survey was done as an anonymous web survey sent as an e-mail containing a link to the web form. According to [49, p. 31], the advantages of this method is that it is fast and many questions can be answered in a relatively short time. The disadvantages is stated as non-representative samples, low percentage of answers, anonymity problems (when using personal e-mail) and technical low quality in questions.

5.4.2 Sample

The receivers of the web survey were selectively chosen by the Information Security Coordinator at NPR, totalling for approximately 25% of the number of employees at NPR. The receivers were persons considered to be most relevant as stakeholders in the following categories: management/staff, section/teamleader, systemgroup (ICT), ordinary employee or hired consultant and others. Many of these respondents had in advance attended the meeting on the measurement of information security and possible advantages. One obvious drawback to this selection of respondents was that not all employees were given the chance to express their opinion with possible loss of important feedback as a result. The cost of including all employees in a survey must also be considered.

5.4.3 Question design

According to [49, p. 37]there are mainly three directions or paradigms in scientific theory that applies when defining the problem and constructing questions in a survey: positivism, hermeneutism and critical theory. Without going further in to these paradigmes, the positivism paradigm is used for most of the questions (objectiv/neutral). In some question the hermeneutic approach is used (possibility for explainations in comment fields) and critical theory (problematization through follow-up questions for respondents signalling a lack of interest in measurements).
Most of the questions were set as 'closed' (predefined alternatives for answering), but some questions were set 'halfopen', with a possibility of selecting 'other' and giving an explanation in a free-text field. The variables in this survey was role in NPR, important area for information security, interest in mesasurenments, and main areas for the measurement of information security (taxonomy).

5.4.4 Questions in the survey

The following questions were presented in the survey:
Question 1: *What is your role in NPR?*
Why ask people which role they have in the organization?
Several reasons exist for this:

- Information need from management and staff should possibly be prioritized compared to needs at a lower level.
- It can be interesting to see if different roles demands information from different areas. (Should we measure only what is interesting for the management, or should we do measurements which are interesting at a lower level in the organization.
- Perhaps there exists a consensus regarding what is important

Question 2: *Which of the following areas do you consider as most important regarding information security at NPR?*
This question was put forth in order establish a foundation to build measurements upon. The assumption is that a large majority of the respondents will consider confidentiality as the most important area. Severe violations of confidentiality of the register will influence the legimity of having NPR as a register with fully identified data subjects. Quality should also be considered as important as this directly influence the purpose of NPR which is mainly health financing and research.
To cover up for all possibilities, two answering alternatives was given - one which attacked the premisse for the question (that information security is important), and that it is possible to rank the different areas according to their importance (confidentiality, availabilty, integrity and quality).

Question 3: *Which areas of information security at NPR do you consider as important to watch closely (measure)?*

This question is very similar to question 2, but multiple choices were allowed for the important areas that should be paid attention to, rather than pinpoint the most important area as stated in question 2. In other words, - is it desirable to do measurements broadly and cover most areas, or should the efforts for measurement be focused on few important areas?
Question 4: *What is your interest in such measurements?*
This is a question that can be difficult to answer immediately for the respondents. Presumably, very few have made up their mind in advantage, and they are now challenged on the potential benefits of measurements and whether they can contribute. The order in which the questions are asked might play a role here, and a rotation of the answering alternatives are done except for the last one. If the respondent answers 'little or no interest', a follow-up question is given in order to find out why.

Question 5 (dependant on Question 4): *You chose 'little / no interest' in question 4. 'What is your interest in such measurements?'. Could you express this more detailed?*

If the respondent states 'little or no interest' in the measurements this follow-up question will try to clearify the reasoning behind this view.

Question 6: *Which of the following areas do you consider most important for information security measurement at NPR?*
This question seek to find the areas considered most important by the respondent. The areas specified is similar to those specified in KITH report R08/04 /cite[p. 20]KITH:

- Human factors
- Technical factors
- Organizational and attitudal factors
- Processes and procedures
- Statistical factors.

Examples of other similar classifications (taxonomies) is given in [25] and [50].
Question 7: *Why do you consider these areas important to watch closely?*

This following-up free text question is logical, but it is also problematic to ask given that reasons for the importance of information security measurements are given in the introduction to the survey. Following this, the question might be regarded as 'leading'.

The survey was done as a web questback survey and was sent to several groups, mainly : Administration/ staff/ management, Section / team leaders, System group and other employees.

5.5 Result of internal survey regarding Information Needs

This section summarizes the results from the internal survey regarding Information Needs. The role of the respondents were distributed as shown in table 1 with most of the respondents being section leaders/ team leaders and from the administration.

Role	percentage
Administration/ staff/ management	33%
Section leader/ team leader	42%
System group	8%
Other employee or hired	17%
Other	0%

Table 1: Role of respondent in survey.

The responses 'Very important', 'Important', 'Less important' and 'Not important' were given weights where 'Very important' = 3, 'Important' = 2 and so forth and the avarage percentage importance score was calculated from all the respondents with 100% being considered most important and 0% not being important at all. The importance from the internal survey is shown in table 2.

Aspect	Importance of area	Importance of measuring
Confidentiality	100%	97%
Integrity	89%	81%
Availability	81%	78%
Quality	92%	92%

Table 2: Aspects of information security at NPR - importance/ importance of measuring

As seen in the table, confidentiality was ranked highest both in importance (100%)and whether it should be measured (97%). Although still important, availability was considered least important of the aspects.

The same method of weighting the scores was applied to the areas that should be measured, and the results are shown in table 3

Area	Importance
Organization/ management	92%
IT Solutions	97%
Physical environment	74%
Personnel	92%
Procedures	82%
Projects	72%

Table 3: Areas of information security at NPR considered as important to watch closely (measure)

As shown, IT Solutions was considered most important to measure, followed by organization/management and procedures.

Finally the respondents were asked what interest they would have in the measurements. As shown in table 4, the respondents were positive to the measurements and found that at least some measurements could be interesting for them.

Interest	Percentage
Little / no interest	0%
No direct interest, but might contribute in providing measurements	0%
Some measurements may be of interest for me / my team / department	58%
Very interesting	42%

Table 4: Degree of interest in measurements

5.6 Measuring confidentiality

Confidentiality of information was ranked as the most important area to watch closely in the internal survey on information needs. This is probably the most difficult aspect of information security to deal with as we seldom know that others 'don't know' and as such it is extreme difficult to measure. In general the confidentiality of health information is threatened by the number and complexity of persons and information systems involved as illustrated in figure 7. The AND functions holds true when all inputs are also true. If there is a confidentiality breach in any system (confidentiality = false on one input), confidentiality for health information has failed as a whole (the output). A discussion on confidentiality requirements can be found in [15].

Ryan & Ryan also states the difficulties with confidentiality [51]

> ...On the other hand, confidentiality is a much less tractable issue than integrity or availability. Compromises of integrity or availability are relatively easy to detect, perhaps using hash functions and auditing access requests. It's possible to compromise confidentiality, leaving few, if any traces, and without changing the compromised information. Moreover, the economic consequences of a confidentiality breach might be difficult to quantify.

Some security measures to protect confidentiality are stated in the NPR regulation[45], like protecting the identity of the patients by encrypting their birth number ('SSN'). The NPR regulation also states how information in the register can be disclosed to other parties (§3). Information disclosures can be of various kinds like anonymous or statistical information and information with deidentified data subjects. After a change in 2009 of the Norwegian Health Research Act[52], information with fully identified data subjects also can be disclosed for research purposes after beeing approved by regional ethical commitees (REK).
One respondent had the opinion that 'it was not of much value to measure confidentiality as they were required[45] [52] to disclose information to several medical research projects which was outside their domain of control'. The information security outside the NPR domain[1] is not a part of the thesis, still there is asked one question in the health trust survey whether research projects are included in the ISMS to give an indication on how information security is handled outside the NPR domain.
Even though confidentiality in itself is difficult (or infeasible?) to measure, security controls which supports confidentiality is implemented and can be measured as such.

[1] As regulated by the security policy

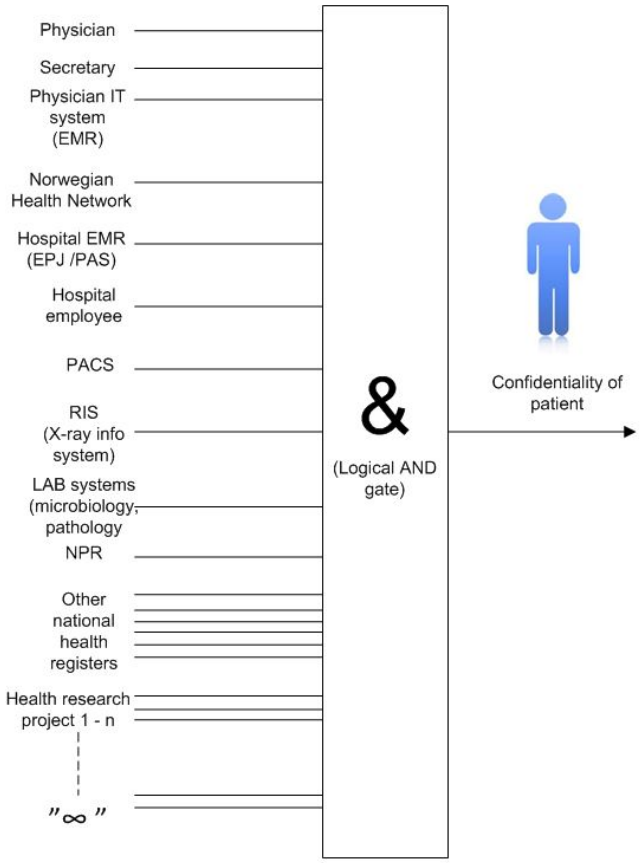

Figure 7: Confidentiality as a logical AND function of all persons and systems involved

6 NPR - Measurement selection and results

This chapter contains the selection of measurements in the case, with an analysis of the cost and validity in the results from the security measurements. The chapter is structured as follows:
The process of selecting measurements is described and how the measurements were implemented. The measurements are accounted for along with a discussion on validity and reliability. Finally the measurements are considered from an economic viewpoint with regard to the cost and the benefits provided. As the 'benefits' are not possible to state in monetary terms (see chapter 'Related Works'), cost-effectiveness is the closest term that can be used (see chapter 'Further Work')

6.1 Existing measurements

Existing measurements at NPR are currently focused at discrepancy reporting. This reporting is included in the annual report to the Data Inspectorate which is required by the NPR Regulation [45].

6.2 Selection of new measurements

The measurements selected came as a result of both customer requests and measurement feasibility. The selection is thus a combination of both the 'Top down' and 'Bottom up' approach for selecting measurements as stated in the KITH report[1, p.10].

In the internal survey, 92 % rated it 'most important' to do measurements of IT solutions like configuration, change, malware, firewalls etc. Also confidentiality was ranked as a top priority so measuring IT solutions from a confidentiality point of view seemed reasonable. The operations of vital parts of the IT infrastructure at NPR is outsourced and a meeting was held with the contractor for the provisioning of measurement data. The following technical measurements where considered feasible and decided to investigate further:

- Number of persons with access to the cryptographic solution for enciphering NPR ident data (E.g.Birthnumber)
- Status for antivirus systems
- Status for security updates and patches for clients and servers / numbers of PCs and servers (from CMDB)

Although internal processes was considered less important to measure with 58% respondant rating it 'Most important', two processes was considered:

- Data reporting to the register by mail (existing measurement)

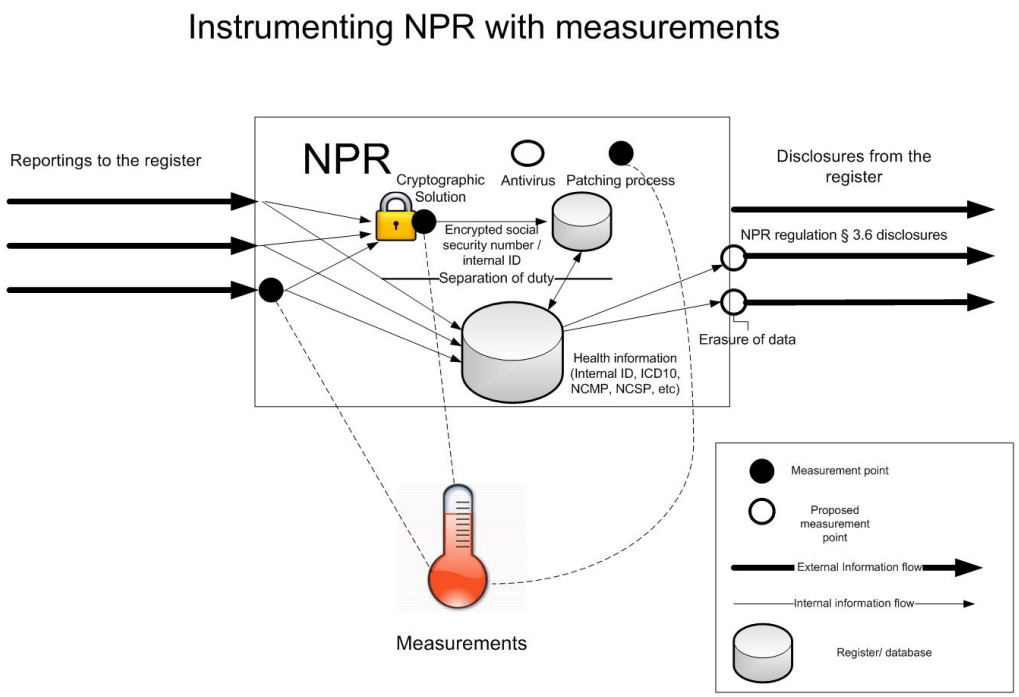

Figure 8: Proposed and performed information security measurements at NPR

- Data disclosed from the register

The reason for this beeing that there existed data for one process (mail reporting) and that there were concerns regarding the confidentiality of data disclosed from the register. Confidentiality of information was ranked by the respondents as the most important aspect of information security (92%). Figure 8 shows the measurements proposed and performed at NPR.

6.3 Economic considerations

As the cost of security breaches on confidentiality is largely unknown in the health sector (See chapter 9- Further research), the economic tools from the litterature were not applied in the case. These could have been used more appropriately if the selected measurements included aspects like availability. In the NPR case, a breach on availability would have been easier to quantify. The measurement costs and benefits are thus stated in textual descriptions.

6.4 Measurement results

6.4.1 Persons with access to decrypt information in the register

The comments on §4.3 (encryption and access to the register)in the NPR regulation [45] states that the number of persons with access to decrypted information in the register should be kept 'low'.

Proposed measurement:

Number of persons with access to the system (cryptographic solution) for decrypting personal information (Birth number /PID)(see 4.6, Data in the NPR).

Results from measurement:

Before measurement, the number of persons with access to the cryptographic solution was expected to be low with just a few persons from NPR and IT operations. After measurements the results suggested that that this number probably was much larger than expected. One explanation could be that instead of beeing treated as a single server with very few persons having access, servers tend to be consolidated and integrated in datacenters where IT operations are highly specialized. This meant specialists belonging to various disciplines of IT operations would need access like:

- Server specialists
- Network specialists
- Storage management specialists
- Backup specialists
- etc.

The result suggests that the increasing complexity of ICT leads to involvment of a number of specialist functions. These key specialists will over time gain privileges across very many systems. Isolation of critical systems with few defined persons having privileges could be a possible solution if this is not acceptable.

Consistency of measurement:

The measurements should be consistent as long as the technical solution along with its authorization system is not altered.

Validity of measurement: Some care should be taken regarding validity of the measurement. People who seemed to be in a position to grant themselves privileges to the system was counted as 'having access'. The validity of this simplification was not verified. Also, only logical access to the cryptographic solution was measured, but physical access should be considered as well for this measurement to be valid.

Costs of measurement:

The case showed that the cost of this measurement is typically the effort to generate a report on useraccounts with access (or possibility to gain access) to the cryptographic solution. This report could be made automatic or done manually. The effort to manually generate a monthly report would typically be 1 hour of labour, while automatic providing the 'raw' measurement data would be two hours with further processing needed. Futher processing/ datapresentation was not done in the case, but this measurement should be possible to do for less than NOK 25.000,- (approx $4000) for the first year with considerable lower costs for the following years if automation is established.

Benefit of measurement:

The benefit of this measurement is knowledge on the number of persons with access to the cryptographic solution. This is useful both for following-up the data controller but also for demonstrating compliance with the NPR regulation[45]. The risk of leaking confidential informa-

tion through misuse of the cryptographic solution by trusted employees is presumedly reduced in inverse ratio by the number of persons having access.[1]. Following the result of this measurement, NPR had to assess whether this number was acceptable.

6.4.2 Status for antivirus/antispyware tools

This measurement was designed for getting status on antivirus and antispyware tools. Such tools should be deployed on all computers and they should have current virus signature files. The contractor for IT operations were contacted in order to estimate which measurements could be implemeted. Unfortunately, this measurement was not implemented during the period of the case study. The reason for this was a change in the underlying computing platform solution at NPR along with a new solution for malware detection. There was also a strong belief from the responsible contractor that there 'had been no malware in this zone - and never would be'. A secure zone does not necessarily guarantee that malware cannot enter - a recent example of this was the damage caused by the Stuxnet malware in isolated zones[53]. This also shows that contractors can be counter-stakeholders in measurements as they will have to both use resources for implementing measurements and the results might trigger further work on their behalf. It can be difficult to transfer all costs associated with this to the customer.

6.4.3 Status for security patches/updates

Proposed measurement:

This measurement was made in order to track the status for security patches and updates. A single measurement was performed manually by getting a status report from the system for updates and software patching. The Configuration Management Database (CMDB)[2] was also queried in order to be able to compare the number of computers in the infrastructure with those in the system for software patching

The measurement revealed the following:

- Many computers lacked 2-3 security upgrades. This was not surprising as there often is a time delay from a patch is received until it is approved, allowing for further distribution in the corporate environment.
- One computer lacked a significant number of upgrades and was subjected to further investigation.
- There were computers not listed in the the patch management system.
- There was a mismatch between the CMDB and the existing configuration at NPR

Consistency of measurement:

The reports from both CMDB and patch management system are assumed to be consistent as long as the technical solution stays the same.

Validity of measurement: Only the status for operating system patches was reported from the patch management system. To get a complete overview of the available patches, the software

[1] Assumption is that logical access is in accordance with the access control system being used

[2] CMDB is a part of infrastructure management as described in the IT Infrastructure Library - ITIL[54]

inventory should have have been scrutinised and relevant patches for each software package identified. For verification of the patching process (and the validity of the measurement), network and vulnerability scanning should have been performed in order to reveal systems not properly registered in the CMDB and for vulnerabilities not patched.

Costs of measurement:

The effort of implementing this measurement was considered low. In the case the measurements were done manually, but spending a few hours would provide automatically reporting of the data. However a more complete system would cost extra, and the same applies for verification of patching through vulnerability scanning.

Benefit of measurement: The mismatch between the number of computers in the CMDB inventory and the number of computers reported from the patch management system triggered an activity of cleaning up the CMDB inventory /patch management system with removing personal computers not longer active in use. Interestingly the CMDB also contained more servers than what was reported from the system for updates and software patches.

6.4.4 Data reporting to the register by mail (existing measurement)

As described earlier, public and private health institutions in Norway are legally required to regularily report their activities to NPR[41][45]. There are more than 2000 entities responsible for reporting, ranging from the largest health trusts to the smallest private contract specialist. For security reasons, the data shall be reported to NPR as two separate files (usually XML), and is typically extracted from the electronic medical records (EMR) found in the hospital systems (EPJ/PAS database). One file contains the *activity data* along with a hospital specific patient ID number. The other file is the *ident file* which contains a mapping between a unique user identification (typically beeing the Norwegian birth number, D-number or similar) with the same hospital specific ID number used in the activity data. The files are sent as separate shipments to NPR

All of the largest hospitals, have started using encrypted electronic transfers through the Norwegian health network (Norsk Helsenett) to NPR, but implementing such systems take time . Some minor public and private health institutions along with many contract specialists mainly rely on postal services for the mailing of removable media (typically a CD/DVD) to the register. These shipments are unencrypted, information security relies on the separation of the ident data and the activity data. NPR has detailed how these shipments should be done and is also measuring how the various institutions comply with these rules. The rules are as follows:

- Activity data and ident data must be sent in two different shipments (two different CD's).
- Each of the shipments must be marked correctly (Ident CD envelope marked with a 'Q')
- Registered mail must be used for the shipments

NPR measures the correct reception of the *activity data* CD's from the largest entities[3]. The discrepancy reporting is done when the following occurs:

1. Ident CD enevelope is not marked correctly with a 'Q'

[3]The smaller institutions consisting of 1600 contract specialists are not measured

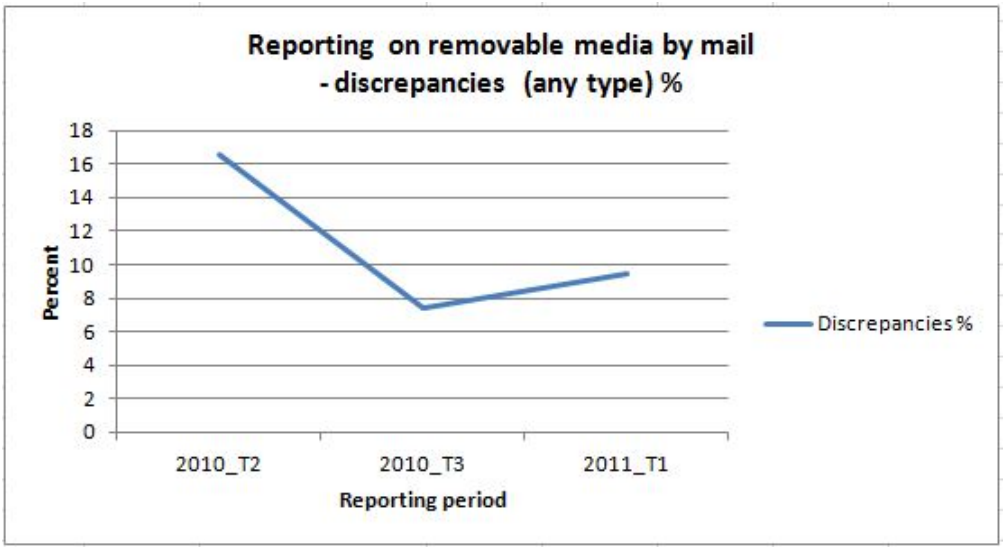

Figure 9: Activity data reporting to NPR on CD - discrepancies in percent of mailings

2. Activity data CD also contains ident data
3. Registered mail is not used

The figure 9 shows how information is reported to NPR. It is important to note that the figure shows only activity data reporting without data from the private contract specialists (the same holds for figure 10 - see further below)

The measurements (see figure 10) shows that there is a decrease in discrepancies over time.

Consistency of measurement:

The measurements are done by manual registration by the departments receiving the CD's and are prone to human error.

Validity of measurement: The measurements are done in order to protect the confidentiality of the information. But what is the threat to this information in the postal system? What makes the use of registered mail safer than ordinay mail? An interview with the head of security for Posten Norge gave the following information:

- Sender has a receipt for the delivery of registered mail and the receiver for the mail is authenticated and has to sign for the reception.
- Shipment is insured for NOK 1.000,-
- Registered mail is sent through the postal system in special plastic envelopes and sealed with security tape[4]
- At arrival the registered mail is separated from the ordinary mail and sorted in a more secure area
- 1.3 million registered mail shipments were performed in 2010. The exact number of lost

[4]This is no guarantee against Man in The Middle (MITM) attacks as tape/plastic bags might be available for criminals

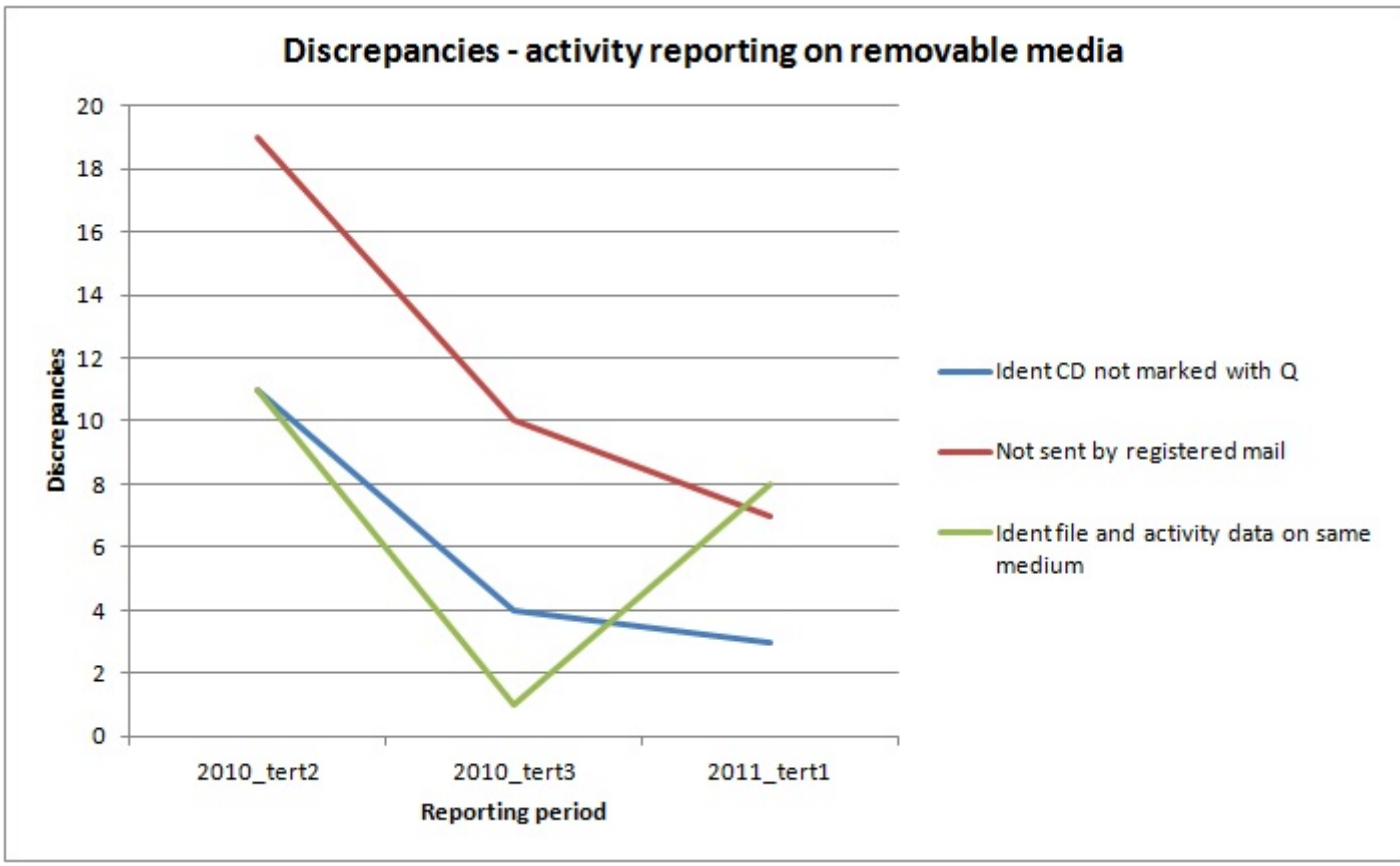

Figure 10: Discrepancies in activity reporting on removable media at NPR

shipments are not made public, but it is in the order of fractions of thousands.[5]

- Registered mail sent from the same place, at the same time (data and ident CD), usually will be packed in the same plastic envelope, and sent to a central terminal for spread sorting. If the mail is sent to the same destination (which is the case for NPR), it is most likely that they will be packed together, but can also be split in separate envelopes. In the (unlikely) event of a registered mail loss, it is likely that both mails (e.g. Ident and data CD) will be lost together.
- The postal service has to date not experienced security breaches by insiders deliberately doing copying of electronic media.
- Encryption is recommended for data media sent through the postal system

Given the amount of CD shipments to the register which is expected to increase from the current level of around 3.000/year to approximately 9.000/year in 2012[6], there is a considerable probability that a mail shipment (both ident and data) will get lost[7]. With the zero-toleranse for confidentiality breaches in the Directorate of Health, the routine for reporting data to the registered should be evaluated further. Possible improvements could be different dates for reporting ident and data, using different postal adresses for ident and data, media encryption etc. The transition to electronic reporting through the Norwegian healt network (Norsk Helsenett) is also a candidate for measurement, as this channel is assumed to be more secure through end-to-end encrypted with PKI.

Costs of measurement:

The gathering of this measurement is done manually and it requires a considerable number of working hours.

6.4.5 Disclosure process

The NPR regulation section 3 deals with the disclosures from the register. §3.6 states that[8]:

1. NPR can, unless otherwise pursuant in this regulation, only disclose personally identifiable data after concession from the Data Inspectorate and in accordance with common rules for professional secrecy
2. For disclosure of personal data for medical and health research, the duty of concession and exemption from professional secrecy is substituted with an advance approval from a regional committee for medical and health research ethics (REK) cf. Health Research act[52] section 33 and 9.
3. Other information disclosures not according to §3-3, §3-4, §3-5 or § 3-7 shall be disclosed in accordance with 1.

[5] For comparison - in 2010 the number of lost Norwegian passports sent as non registered (ordinary) mail was 537 out of approx. 600.000 equal to 0.0895% of the mailings[55]

[6] Increase is caused by contract specialists, which from 2012 will have to report every fourth month instead of yearly - this number is then expected to decrease as electronic reporting through NHN becomes more commonplace

[7] A Monte Carlo simulation could prove useful here to estimate the risk

[8] Authors own translation of the NPR regulation

Sometimes an inquiry for deidentified data according to §3.4 in NPR leads to a new application for a §3.6 disclosure containing fully identifiable personal data[9]. These disclosures are regularily reported in the compulsory annual reporting from NPR to the Data Inspectorate, but the thought was that it could be interesting for the Data Inspectorate to get a more detailed specification. By showing the volume of personal data in each disclosure with a free text describing the type of data, the Data Inspectorate would get a clearer picture of the dataflow *from* the register. When informally contacted, the Data Inspectorate could not confirm or de-confirm that this information was of interest to (or required by) them as this would have to go through a formal process.

Costs of measurement:

The cost for producing these numbers are low, as these can easily be gathered when data is extracted from the register.

Benefit of measurement:

According to [10], security measurements (metrics) should facilitate insite for decission making. The problem with this proposed measurement is that it does not help in decission making at NPR. The register can do a 100% job in protecting confidentiality of personal health infomation, but when the regional ethical committees (REK) give an approval for disclosure of personal health information, this information will flow from NPR to medical or health research project. Although the 'Code of Conduct for information security in the healthcare, care, and social services sector'[12] recently has published recommendations for dealing with information security in medical and health research projects (Fact sheet no. 40 with an accompanying guidance document), it is unclear how good this information is known and used for securing information in research projects. Logging access to persons medical records is not described in this fact sheet[10]. This information could prove to be interesting for the Data Inspectorate when planning supervisions but this was, as discussed earlier, not confirmed.

Erasure of disclosed data

It is important for the register that disclosed data is erased when the purpose of the data is fulfilled. The entity receiving disclosed data signs a formal agreement with the register where they are required to confirm the deletion of data on a special form. This measurement was proposed in order to track the outstanding data and make sure the confirmations on deletion of data was returned in a timely manner(According to ISO 27004).

Costs of measurement:

The cost for producing these numbers are low, as the date for erasure of disclosed data can easily be tracked with a calender function.

Consistency of measurement:

The measurements are done by manual registration by employees at NPR and thus prone to human error.

Validity of measurement:

[9]Several pathways exists here, instead of beeing a new application for §3.6 data, fewer variables might be agreed upon or NPR generate statistics themselves

[10]Access to medical records in hospitals are recorded in the EMR (EPJ/PAS) system, but little is known about logging access to similar information in research projects. There exist however advisories on protecting the file containing the research subjects (separated from research file containing the actual data)

The problem with ensuring erasure of disclosed data is that some research projects are long-term (lasting 10 years or more). In this amount of time, the organization, personell and procedures at NPR might change significantly and it is vital that the measurements 'survive' these changes.

6.5 Data Analysis and Discussion

Lessons learned from the case related to the research questions:

Measurements seems to be costeffective when carefully selected (cost compared to presumed value although not stated in monetary terms)
Measurements with low cost can be found that provides high value (even manually performed measurements)
Validity is a challenge when implenting measurements, it is hard to measure exact the properties wanted. Although not 100% valid, measurements still provide useful information for decission making.

Further lessons from the case:
Deciding on measurements is probably easier when an operating ISMS (eg. ISO/IEC 27001[30]) is in place with its controls and a formal risk analysis has been done beforehand. However the progress of implementing security e.g. implementing ISMS, performing risk analysis can itself be subject to measurement.
Discussing implementation of measurements might trigger other necessary processes in an organization (e.g changing working procedures, performing risk analysis etc.)
Change is a threat to existing information security measurements if these are not integrated in the change processes (e.g. Implementing a new antivirus solution might not report status if measurements are not taken account of in the project)[11]. Frequent changes might destroy continuity in the measurements (and historical data)
Information security measurements should be negotiated as a part of outsourcing contracts. [12]
Measurements are difficult to implement when information traverses different entities (enterprise domains).Confidentiality depends on all parties involved with the transferring and processing of medical information.

[11] Standards for automatic information exchange of security measurements like the The Security Content Automation Protocol (SCAP)[56] might be helpful
[12] Costs for measurements will probably increase if they are deployed after signing the outsourcing contract.

7 Health trusts survey - design

This chapter contains the design of a survey on information security measurements in Norwegian specialist health care and is structured as follows: First the population and respondents in the survey are discussed. Secondly the design of the questions is discussed along with a pilot on the survey. Finally the actual implementation of the survey is shown.

7.1 Population and respondents

The population of the survey was chosen to be 'Persons with *responsibility for* or *strongly involved with* information security in Norwegian Hospital trusts, with a few respondents also from private health institutions and governmental health registers. Typically these are people appointed to represent the various health trusts in the information security forums conducted by the respective health authorities (RHF's). Respondents was mainly gathered from sources like internal auditing departments or information security departments in the RHF's but also from known participants in these forums. Typical job titles for respondents would be 'Information security leader' or 'Information security coordinator'. Sometimes these roles are also combined with beeing an Data Protection Official/Officer (personvernombud). The advantage of asking these respondents is that they are likely to possess information about information security which is a prerequisite for asking further questions regarding measurements. The drawback is that conclusions will be limitied to this group. A true random selection would have been the ideal, but was not considered possible given the small population.
As this population is rather small with 26 hospital trusts in total[1], all the hospital trusts were intended to be asked in the survey.

7.2 Question Design

This section describes how the questions were designed. An introduction to measurement of information security is given at the start of the survey. Here it is also stated that performing measurements are not compulsory according to the "Code of conduct for information security in the health sector" [12]. Hopefully this makes it easier for respondents to be honest in their responses, knowing that they have not violated any laws, regulations or 'best practices'. It is important for the validity of the survey that the responses are as correct and representative as possible. The scientific reasons and purpose for asking the questions in the survey is also stated. The introductory questions are in the positivism paradigm[49, p.39].
First some background variables (demographics) are asked:

What is your sex?
This question is only used for describing the respondent

[1] As of Sep. 2011 - the number is constantly changing with the trend of merging smaller hospital trusts into larger trusts

What is your age?
Together with the previous question, the answers will give a description of the typical respondent.

To which Regional Health Authority (RHF) or other category does your organization belong?
Besides further describing the respondents, this question will enable comparisons between the Regional Health Authorities (RHF's)given enough respondents.

How many employees are there in your health trust or organization?
From sample annual reports from the regional health authorities (RHF) some of the greatest hospital trusts in Norway employs more than 5000 persons and some of the smaller trusts below 2000 persons. The categories are thus divided into small hospital trusts (<2000 employees), medium (2000-5000 employees) and large (> 5000 employees) in order to spread the results.
The larger the health institution is, the more likely it is that it has dedicated people working with information security. After all, large organizations do more of 'everything'[37, p. 47] and the expectation is that at least the larger hospital trusts have dedicated people working in this area.
The pharmacies associated with the hospitals in each region are also organized as hospital trusts but the number of employees are typical much smaller than at the hospitals. Due to their small size, some of these pharmacy trusts are expected to have limited resources when it comes to information security.

How large part of your position is dedicated to working with information security?
This question is mainly asked as a background variable but there is also an underlying assumption that the largest health enterprises have persons dedicated to information security. Aligned, with both the previous and next question, it will be possible to assess how the various enterprises are staffing the information security function and thus giving it priority.

How many (total) in the enterprise works full-time (dedicated) with information security?
The reason for asking this question is the assumption that the largest enterprises have at least one or more persons dedicated to working with information security.

Has a goal for information security been established in the organization?
This question seeks to discover whether information security goals are established in the organization. Having established security goals are compulsory according to the 'Regulations on the processing of personal data (Personopplysningsforskriften)[47] and the 'Code'[12]. This question is thus measuring one important aspect of *compliance* in the organization.

Does your organisation measure information security?
The question is similar to the question used in a survey on information security metrics performed

by Bakås in 2005 [13]. In this survey, 67% of the respondents stated that they were measuring information security, but in the public service sector only 29% was doing measurements. The assumption is that measurements in hospital trusts are rare and it is expected to score equal to or below this number given the resource constraints in the health sector. A follow-up question qould have been implemented in the critical theory paradigm[49, p.44] like 'What keeps you from measuring information security?', but this was not implemeted in order to limit the extension of the survey.

To which degree do you know /are you familiar with the following documents /standards for information security mesasurements? State this on a scale from 1 to 4 where 1- Very acquainted with 2- Basic knowledge 3 - Some knowledge 4 - No knowledge
The next section asks which standards or publications the respondent knows about in order to gain knowledge on whether the measurements are rooted in systematic approaches from litterature. A special report on information security measurements was published by the Norwegian Centre for Informatics in Health and Social Care (KITH) in 2004 [1] and it is unclear to which degree this report is known or has had an influence on measurements in hospital trusts. In [13, p. 31], more than 50% of respondents measuring information security used status surveys from ISF [34]as a tool. Common tools from ISF are *ISF Benchmark* (former Security Status Survey) and *Fundamental Information Risk Management (FIRM)*.
The NIST special publication SP 800-55 "*Performance Measurement Guide for Information Security*" [7], first published in 2003 and revised in 2008, provides guidelines for information security mesasurements. The SP 800 series is frequently referenced in the litterature and should be well known by IS professionals. The *ISO/IEC 27004* standard was published in 2009 and is at the time of this writing fairly new and presumably not very well known. Other ISO standards in the 2700X series like the ISO 27001 and 27002 standards have been around for a longer time and are more known.[2]

To which degree do you agree or disagree to the following assertions - state on a scale from 1 to 4 where 1 - Strongly agree 4 - Strongly Disagree

The next section of the survey is designed to measure attitudes concerning information security measurements and the questions asked is in the hermeneutic paradigm[49, p.41]. The risk of introducing bias in these questions are considerable. Some of the claims regarding security measurements are negative towards measurements while others are positive and the order in which they are presented may influence the responses. To counter this, the claims are presented in random order for the respondents.

- Respondents are asked to state their opinion on the claim 'measurements of information security is not worthwhile'. There are several reasons for believing measurements are unnecessary, one could be that the controls are considered so good that this is redundant, another

[2]Using a trend service e.g. trends.google.com against the various ISO standards will verify this

that they are not costeffective. It could also be that there are so many different areas to measure making it impossible to pick the right ones.

- ISO standards are very formal of nature.This can be an obstacle for implementing them and ISO27004 have recently been criticized [57] for 'having little prospect for achieving the goal'. The claim 'ISO standards are difficult to understand or implement' is thus put forward.
- A claim on costs of measuring information security is provided ('It is costly to measure information security'). The word costly has a very low precision - do we mean 'cost a lot of money' in absolute monetary terms or that the cost is larger than what we are willing to pay? The question is still included although its validity may be low.
- In order to get more knowledge on the reasons for measuring, the claim 'Measurements are requested by management' is put forward. In [13, p.33] there is a strong correlation between measurements and demand from management and this question might confirm that the same holds for Norwegian hospital trusts as well.
- Outsourcing IT services are very common and the Norwegian regional helth authorities (RHF's) have organized their IT operations in fully owned subsidiaries. It could prove valuable for the hospital trusts to have security measurements reported as part of their Service level Agreements(SLA) with their IT suppliers. Respondents are asked to which degree they agree that security measurements should be included in their SLA's.
- Quality indicators are used in specialist health care[58], but none so far includes information security. Should also reporting on information security (e.g. uptime on system with electronic health records) be done as well?
- The importance of watching closely how information security develops over time is stated. Probably very few respondents will disagree to this. This statement may have potential to give bias in the survey because it explains the purpose of measurements.
- Regulary reporting of information security status is believed to be habitual for organization measuring information security.
- The 'Code of conduct for information security in the health sector' [12] does not include measurements of information security in its current version. Respondents are asked whether such an amendment should be considered.

Have status for the work with information security been reviewed by senior management in 2010?

The next question is in itself a measurement of information security practices in Norwegian Hospital Trusts. Asking whether the status for information security has been reviewed by senior management indicates how close the organization follows a practice which is mandatory according to the 'Factsheet 2 - ISMS' in the 'Code of conduct for information security in the health sector'[59]. For further verification of the answers, the date for this review is also asked.
If the management review has taken place, the respondents are also asked which areas have been part of the review:

Which areas have been included in the review?
Multiple choices are available for selection:

- Information Security Management System (ISMS)
- Reported discrepancies /security incidents
- Status for risk analysis
- Measures to improve information security
- Education (employee awareness program)
- Security revisions

It is also interesting to know which ISMS the organization uses and asking this question will provide more knowledge on this issue. Health organizations using the ISO/IEC 27001[30] will have an advantage when implementing the ISO/IEC 27004 [8] measurement standard as the latter is designed to be used with the ISO/IEC 27001. **Which standard(s) are used for managing information security?**
The following standards are available for selection by the respondent:

- Company specific ISMS (non-standard)
- ISMS based on 'the Code'
- ISO/IEC 27002
- ISO/IEC 27001
- ITIL (IT Infrastructure Library)
- COBIT (Control Objectives for Information and related Technology)
- Other standard

Are research projects also encompassed by the information security management system (ISMS)
This question is asked in order to see what the respondents practices or think about having research projects within the ISMS. If they are not encompassed by the ISMS, chances are that information security is left at the will of the project leader. If not encompassed it is also crucial that the Regional Ethical Comittees (REK) carefully scrutinize the research applications. The Data Inspectorate is sceptical how REK is performing in this area and have identified several challenges[60, p.10].

The last two questions are the same as those used in the internal survey at NPR, see chapter 5.4.4:

Which aspects of information security do you think is most important to whatch closely?

State on a scale from 1-4 where 1 is Very important 2 is Important 3 is Less important 4 is Not important
The choices are:

- Confidentiality (information is available only to authorized users)
- Integrity (information secured against unintentionally or unauthorized changes)
- Availability (Information is available when demanded)
- Quality (Correct information is registered in the system)

According to [43], health information used beyond the appointed medical treatment could be named secondary purposes for processing data. NPR is a typical user of health information for secondary purposes. The assumption is that the institutions directly involved in patient treatment will rank the availability of information highest. As an example, surgical procedures are often postponed when electronic health records (EHR) are unavailable. The correctness of the information is also vital and integrity and quality of the data is expected to be considered important. There might be a different opinion on the importance of confidentiality between psyciatry and general (medical and surgical) medicine.

State how important you consider information security measurements in areas stated below (examples are provided) 1 is Very important 2 is Important 3 is Less important 4 is Not important

State which areas considered most important for information security measurement?
The taxonomy is also the same as used for the NPR internal survey:

- Organization/management (compliance, risk analysis, discrepancies, authorizations, correcting efforts)
- IT solutions (configuration, change, security measures, firewalls, antivirus etc.)
- Physical environment (Perimeter security, locks, lockers, fire prevention, power supply etc.)
- Personell (Security awareness programs, attitudes)
- Work procedures
- Projects (information security in)
- Other areas

7.3 Pilot on Survey

Before launching the survey, it was sent to two different persons working in the field to get feedback on the question formulation and on the survey as a whole. From the feedback, only some minor adjustment of the questions were done to make them more comprehensible (grammar and making a few terms more precise). A better pilot could have been performed by using a larger group of respondents, but this was considered as impractical given the population size and time available.

7.4 Questions asked

The questions discussed in this chapter was implemented as a web survey as shown in Appendix B (Norwegian only).

8 Health trust survey - findings

This chapter contains the results from the survey on information security measurements in Norwegian specialist health care. This chapter is structured as follows: First a discussion on validity and reliability is performed followed by a description of the respondents of the survey (background variables). Then the results from the survey is presented along with an interpretation.

8.1 The respondents

The survey was mainly conducted in the hospital trusts (HF's) owned by the four Norwegian Regional Health Authorities (RHF's)[1] but also respondents from private health institutions and government health registers were includeded. The survey was sent as a web survey by e-mail to 33 security practioners responsible for, or working with information security. The participants was chosen from the four Norwegian health trusts (78.8%) , with a few respondents from private health institutions (12.1%)and governmental health registers (9.1%).
Of these, 16 respondents completed the survey (48%), plus one incomplete response (3%).

8.2 Validity and reliability

Ideally the selection should be a representative sample of all information security practioners in Norwegian health care, making it possible to do inferential statistics from the results into the whole population. However it is not that simple, mainly because of *self-selection* - the respondents chose themselves (or was permitted by their leaders) to answer the survey[2]. Although this was addressed in the survey design by trying to actively choose the respondents, there is not sufficient evidence that the respondents are representative.This hinders the use of more advanced statistical methods on the findings, and statistical testing of the nul-hypothesises are thus not performed.
Self-selection is also a problem in well known security surveys as in the '2010 / 2011 CSI Computer Crime and Security Survey'[38] having a response rate of 6.4 % from 5412 possible respondents. The CSI Survey also states that individuals and organizations that have actively demonstrated an interest in security are more likely to answer, leading to bias.
When asking three respondents who chose *not* to participate in the survey, they stated the following reasons:

- 'too busy'
- 'formal reasons - the survey should have started with a formal application for participating from the researchers college'

[1] Although owned by the RHF's, the hospital trusts are responsibe for their own information security as data controllers[46].
[2] This is discussed in Shostack and Stewart[37, p.46]

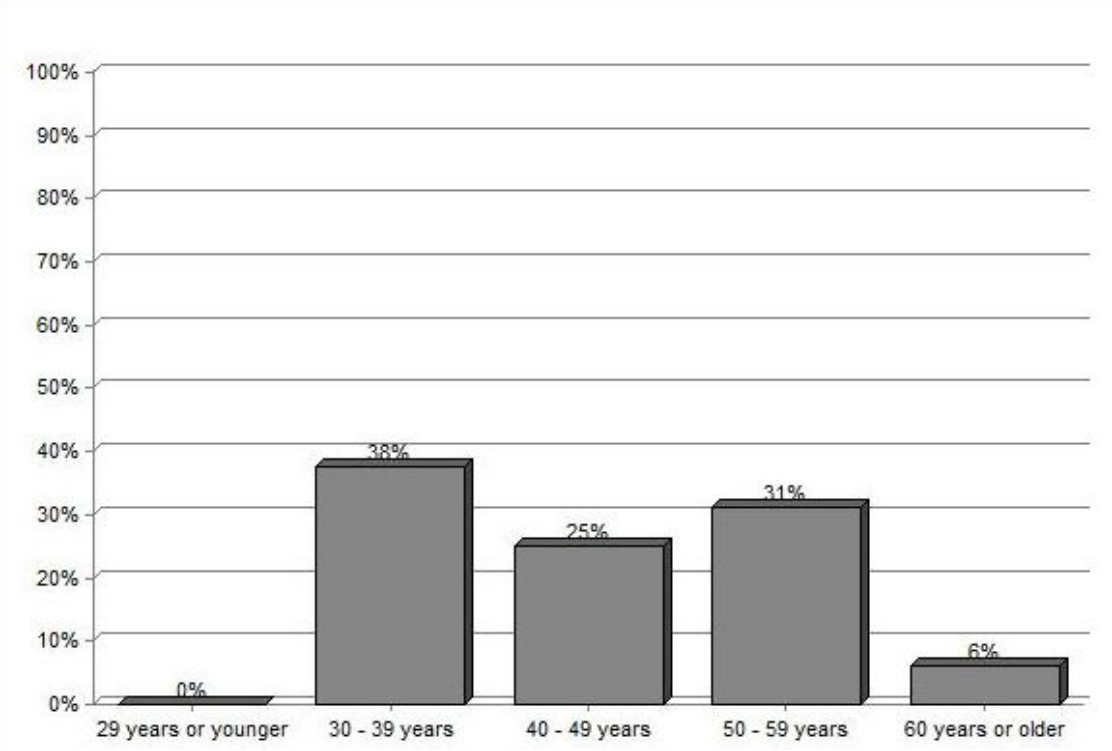

Figure 11: Respondents - age distribution

- 'poor survey design: mapping the status for health trusts is mixed together with asking for personal attitudes from the respondent.'

If these reasons for not participating in the survey are representative, then the bias in the survey caused by the self-selection should be low, but care should be taken when interpreting the results since people in general are unwilling to talk about security failures[37].
The last reason for not participating in the survey is interesting, pointing towards that there may be differences in the respondents personal opinion versus that of corporate management. Some of the survey questions was not designed with this in mind.

8.3 Background variables

The average respondent in the survey was found to be a male person in the interval 40 - 49 years, however the most frequent observed respondent was found to be in the interval 30 to 39 years old. Figure 11 shows the age distribution of the respondents. Respondents from health trusts in all Norwegian regional health authorities (RHF) were represented in the survey, but as there were too few respondents (16 in total), the results were not broken further down to show differences between the four health authorities.

Figure 12 shows the RHF and other category that the respondent belongs to.

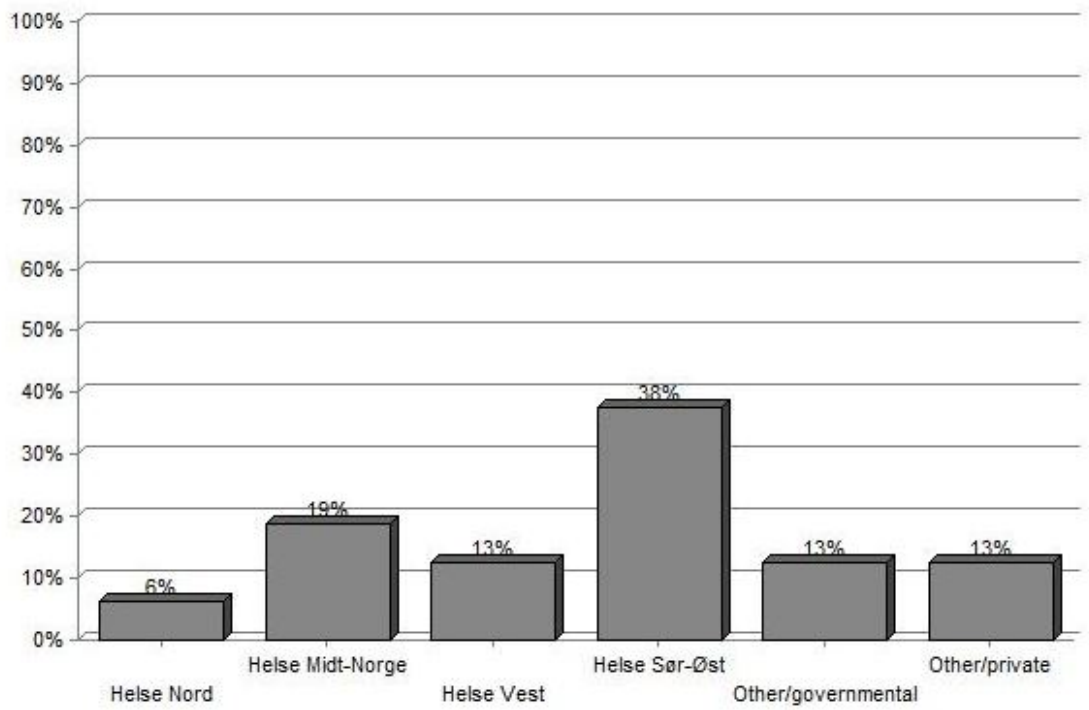

Figure 12: Distribution of respondents in the Regional Health Authorities / others

Size of organization	Percentage	Respondents
Large health trust/organization (> 5000 employees)	50%	8
Medium health trust/organization (2000 - 5000 employees)	0%	0
Smaller health trust/organization (200 - 2000 employees)	38%	6
Small health trust /organization (< 200 employees)	12%	2
Total	100%	16

Table 5: Respondent distribution according to size of organization

Part of respondents position dedicated to working with information security	Percentage	Respondents
Full time (100%)	31%	5
Part time (20 - 99%)	25%	4
Smaller part of position (5 -20%)	25%	4
Information security not a daily task (less than 5%)	19%	3
Total	100%	16

Table 6: Part of respondents position dedicated to working with information security

8.3.1 Number of employees in organization

Table 5 shows the distribution of respondents with regard to the size of the organizations. There were none respondents in the 2000-5000 employees category.

8.3.2 Part of position dedicated to working with information security

In the survey, 31% of the respondents were full time information security professionals with another 50% working part time or smaller part of position with information security (see table6). The respondents working full time were expected to work in the largest enterprises, but surprisingly the numbers was almost the same for the large health trusts (> 5000 employees - 38%) and the smaller ones (200-2000 employees - 33 %). None of the smaller organizations (<200 persons) in the survey had persons dedicated to working with information security.

8.3.3 Total persons in enterprise working with information security

The distibution of persons working full time with information was as shown in table 7.

It was expected that the largest health trusts (>5000 employees) had persons dedicated to working with information security. However, the results from the survey showed that as much as 38% of these had no persons dedicated to working with information security. 25% of these enterprises had one dedicated person and another 25% had dedicated persons in the interval 2-5 employees. None of the smallest enterprises (<200 persons) had dedicated people working with information security. This suggest that the focus on information security varies amongst the health enterprises, or at least major differencies in how the work with information security is organized.

Number of security practioners in the enterprise (full time position)	Percentage	Respondents
None	56%	9
1 person	19%	3
2-5 persons	19%	3
6 or more persons	0%	0
Don't know	6%	1
Total	100%	16

Table 7: Number of full time security practioners in respondents organization

Goal for information security established in the organization	Percentage	Respondents
Yes	75%	12
No	13%	2
Don't know	13%	2
Total	100%	16

Table 8: Goal for information security established in the organization

8.4 Establishment of goal for information security

Table 8 shows the respondents response to whether a goal for information security has been established or not. A goal was stated as a 'formal policy' for information security or other document with security objectives.

All large organizations (100%) were found to have established a goal for information security. Only half (50%)[3] of the smaller /smallest organizations (<2000 employees) have established this. This is not in accordance with the 'Regulations on the processing of personal data' (Personopplysningsforskriften)[47], which in section 2, 3rd paragraph states that 'The purpose of the processing of personal data and paramount objectives for the use of information technology, shall be described in security goals'[4].

8.5 Measurements of information security in the organization

In the survey, 56% answered that they were measuring information security (see table 9. This number is higher than expected from the survey on measurement practices performed in 2005 [13, p.25] where 29 % of the respondents of the respondents in the public sector stated that they were performing measurements of information security. Although there were few respondents from the public sector in the 2005 survey, the numbers suggest that it is now more common to do such measurements and this was not expected.

It is interesting though, that two of the respondents measured information security without knowing or having a stated goal for information security in the organization.

[3] 'don't know' responses is counted as 'not in place'

[4] Authors own translation of the regulation

Measurement of information security performed in the organization	Percentage	Respondents
Yes	56%	9
No	44%	7
Don't know	0%	0
Total	100%	16

Table 9: Organizations measuring information security

8.6 Familiarity with information measurement standards

The familiarity with measurement standards are shown in figure 13. The initial assumption was that there is little knowledge on information security measurement standards in Norwegian hospital trusts. The results show that the best known standards (some knowledge or better) are the KITH R08-04 (62%) report[1] and ISO/IEC 27004(56%) which is promising given that it is only 2 years old at the time of the writing. When the results of 'knowledge of measurement standards' are crossed with 'measurements performed in the organization', the numbers of organizations performing measurements are larger (than the respondents with basic or better knowledge of measurement standard (this applies for all standards). This leads to the assumption that some organizations measure information security without a basic understanding of measurement standards.

8.7 Opinon on assertions regarding information security measurements

Figure 14 shows the respondent opinion on assertions regarding information security measurements. From the results the following can be stated:
88 % of the respondents have the opinion that information security measurements are worthwile (disagree or strongly disagree with the opposite assertion that they are *not* worthwhile).
The majority (69 %) also, at least partly, agrees to the statement that ISO standards are difficult to comprehend or implement. This might be an obstacle for implementing standards like the ISO/IEC 27004[8], confirming the criticism by Hinson[57] that the standard is 'too academic and complex'.
The majority of the respondents (75%) believes that the benefits outweighs the cost of performing measurements (partly or strongly disagrees to the assertion that cost is larger than the benefits).
Only one respondent (6%) partly agrees to the statement that measurements are requested by management while the rest (94%) partly or strongly disagrees. This suggests that information security measurements is not at the top on the agenda of management[5]. One possible explanation for this presumable 'lack of interest' in information security could be that the IT systems mostly are stable and few (at least public) security breaches occur.
A large majority of the respondents (81%) agree that information security measurements should be a part of the enterprise SLA (Service Level Agreement) contracts. The need for information

[5]The lack of interest in information security from leaders was recently (nov 2011) adressed by the Norwegian Defence Minister Espen Barth Eide[61]. He also stated a need for leaders who prioritize security and the difficulties involved with building a security culture, if not prioritized by management

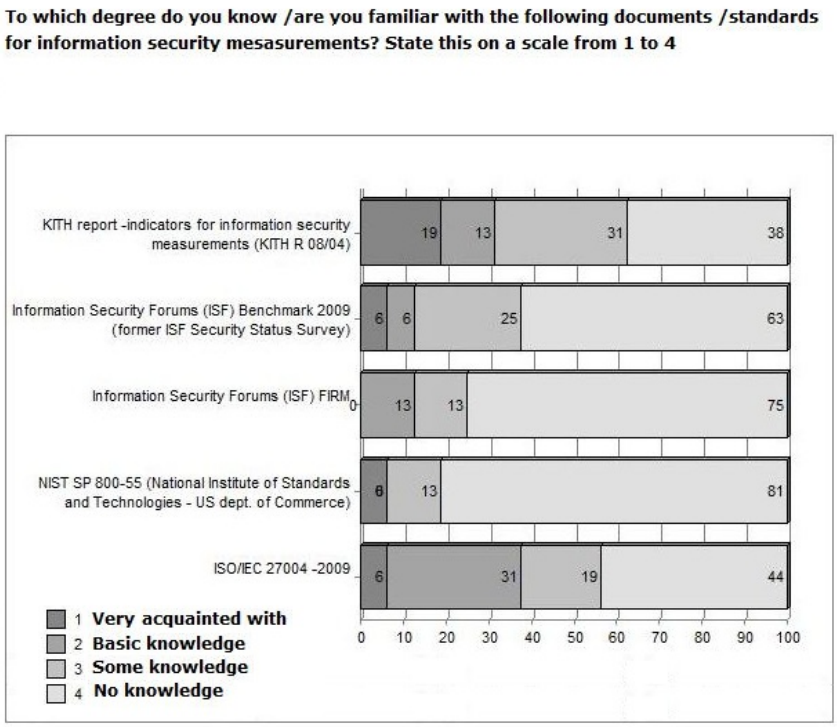

Figure 13: Respondents knowledge regarding information security measurements standards

security in SLA is adressed in various standards and guides like the NORSIS guidance on IT outsourcing [62], but often the measurements of information security are limited to uptime or system stability.

On the assertion 'Measurements of information security should be reported with other quality indicators from the enterprise', as many as 84% partly or strongly agrees that these should be included. If certain measurements are made compulsory, the status for information security will be more visible and, perhaps, getting more attention from management. Currently, security is not included in the national quality indicators for specialist health care, but 'safety and security' is descibed as an area in the aspects of good quality[58, p.8].

The vast majority (88%)of the respondents strongly agreed to the statement that it is 'important to watch how information security evolves over time'. This was expected and the response is very similar to the statement on whether measurements of information security are worthwhile.

Even though security measurements are not requested, the majority of the respondents still regularily reports this to senior management.

Measurements of information is currently not a part of the 'Code of Conduct for information security in the healthcare, care, and social services sector'[12]. 88 % of the respondents partly or strongly agrees that 'the Code' should encompass this. Such measurements could also provide

the basis for quality indicators on information security.

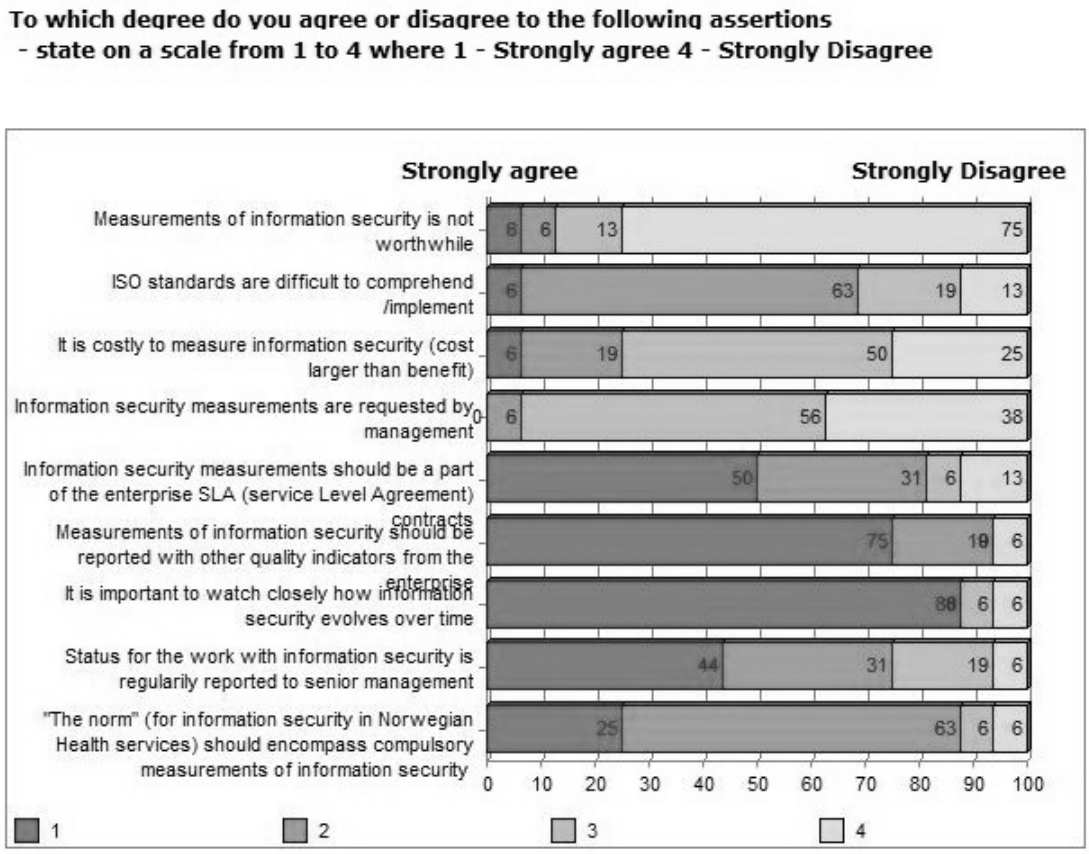

Figure 14: Respondents response to assertions regarding information security measurements

8.8 Information security status - review by senior management

The demands for implementing an Information Security Management System (ISMS) in 'the Code'[12][6] states the following:

> The management review must be conducted in accordance with the established agenda. The purpose of management review is to uncover whether security is maintained with regards to objectives, strategies, procedures, and adopted action plans for further work with security. Management review must at minimum be conducted annually and in connection with financial or activity planning.

Table 10 shows that 69% of the respondents review information security status annually, in accordance with the demands/recommendations in 'the Code'. For verification, the respondents were also challenged to state the date for this review. Two respondents stated the exact date, further two respondents stated the month for review while as many as seven respondents chose

[6] Supporting document Fact sheet no 2 - 'Control system for information security'

to skip the question. It is thus reason to believe that not all health trusts operate their ISMS in fully compliance with the code and the formality of management reviews can also be questioned.

Status of information security reviewed by senior management in 2012	Percentage	Respondents
Yes	69%	11
No	25%	4
Don't know	6%	1
Total	100%	16

Table 10: Informations security status - senior management review 2010

8.9 Areas included in Information security status reviews

The respondents who stated that they reviewed information security annually where also asked which areas these reviews included. The figure 15 shows that most of the relevant areas were included in the reviews. Information security auditing were included in almost all reviews - suggesting that information security auditing is an area management pay attention to.

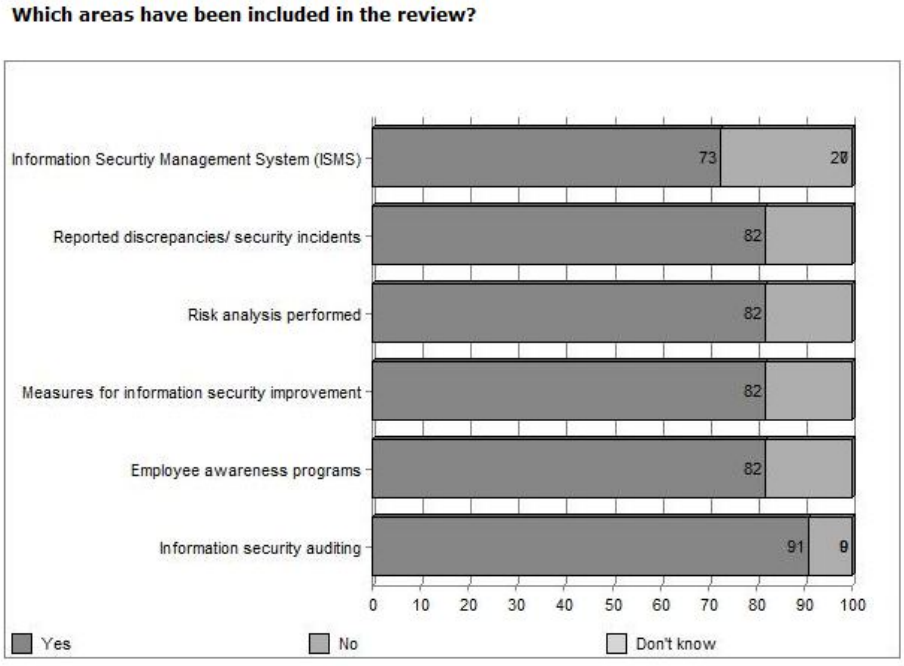

Figure 15: Areas included in senior management review 2010

8.10 Standards used for managing information security

As shown in table 11, all respondents stated that they used 'the Code' as a standard for implemeting an Information Security Management System (ISMS), thus showing the importance of the Code[12] as a guideline for managing information security. Further 50% had implemented their

Standards used for managing information security	Percentage	Respondents
Own system for managing	50%	8
Based on 'the Code'	100%	16
ISO/IEC 27002	0%	0
ISO/IEC 27001	0%	0
ITIL (IT Infrastructure Library)	19%	3
COBIT	0%	0

Table 11: Standards used for information security management

Research projects encompassed by the ISMS?	Percentage	Respondents
Yes, encompassed and included in management system	56%	9
No, information security in research projects is the responsibility of the project leader	31%	5
No, but the management system will be extended to encompass these	0%	0
Don't know	6%	1
Not relevant	0%	0
Other / comments	6%	1
Total	100%	16

Table 12: Research projects encompassed by ISMS

own ISMS with basis in 'the Code'. Of the other standards, 3 respondents stated that they used ITIL and one respondent used ISO/IEC 27001[7].

8.11 Inclusion of research projects in ISMS

As shown in table 12, most organizations (56%) include research projects in their ISMS. 31% stated that that this was the responsibility of the project leader. One of the respondents stated that research projects had their own internal control system[8]. These numbers suggests that the Regional Ethical Comittees for research projects (REK) should pay close attention to how information security is ensured in applications for the approval of medical research projects. Even though the research is done in a health trust with an ISMS in place, it should not be taken for granted that the information security will be taken care of by the ISMS.

8.12 Measurement of important aspects of information security

Although all aspects of information security are considered very important to measure by the respondents (see 16), the *integrity* aspect is rated as the most important by all respondents (100 %) closely followed by *quality* (88%) and *availability* (81%). Although *confidentiality* is still considered by most respondents as very important, it is ranked as the least important aspect of information security.

[7]Which is the basis for implemeting the ISO/IEC 27004 security measurement standard
[8]As stated in the Health Research Act [52]

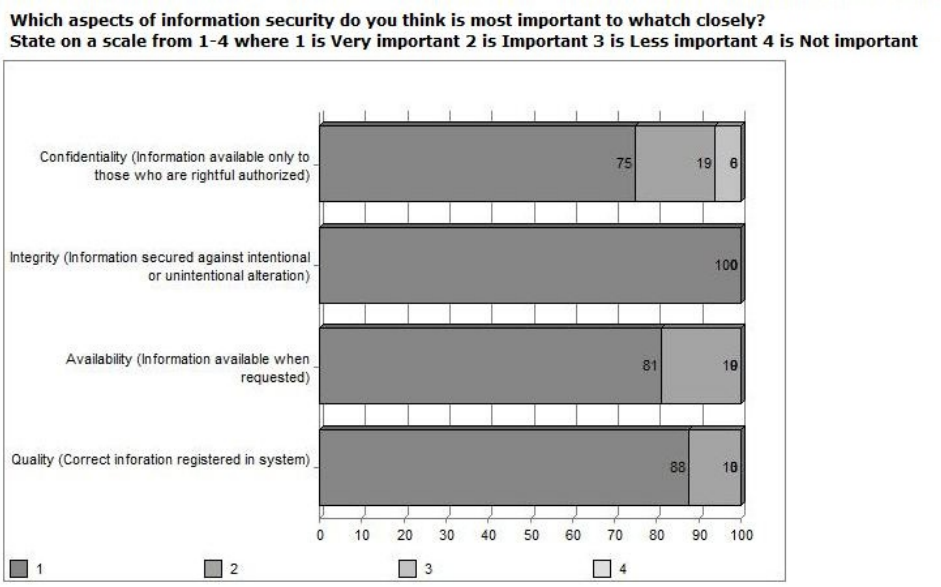

Figure 16: Aspects of information security - importance

8.13 Measurement of information security areas

The respondents opinion on the importance of measuring various areas are shown in figure 17. Technical solutions were ranked highest in importance with 81 % considering it 'Very important'. Personnel (75%) was ranked as the second most important closely followed by procedures (69%).

8.14 Comparison with results from the NPR internal survey

The same questions on the importance of various aspects and areas were asked in the NPR internal survey in the case study. An interesting comparison can be done by correlating the percentages of the respondents answers to aspects considered 'very important' and 'important'. The correlation coefficient was calculated by using the simple correlation equation:[63, p.427]

$$r \equiv \frac{\sum xy}{\sqrt{\sum x^2} + \sqrt{\sum y^2}}$$

Where $x = X_i - \bar{x}$ is from the percentages in the NPR internal survey and $y = Y_i - \bar{y}$ taken from the survey in the health trusts.

As shown in figure 18, a strong positive correlation was found between the survey in the health trusts and the NPR internal survey regarding areas 'Very important'(0.93) and 'Important to measure'(0.92). This suggests that there is a consensus of which areas that should be prioritized for measurements in the health sector ranked as follows:

1. IT Solutions
2. Personnel

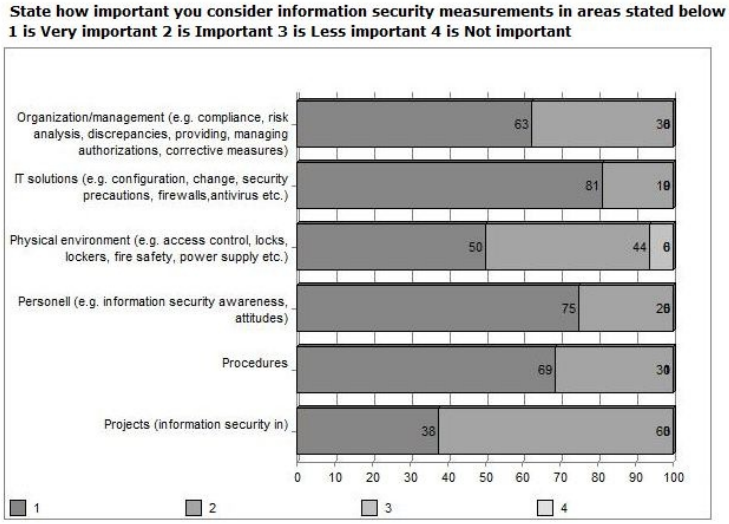

Figure 17: Importance of measuring information security areas

3. Organization/management
4. Working procedures
5. Physical environment
6. Projects

It is also interesting to note that opinions differs strongly between respondents from the health trusts and respondents in the NPR internal survey regarding the importance of various aspects of information security. Figure 19 shows the disagreement with a strong negative correlation between the opinions (-0.82 for aspects considered most important and -0.84 for aspects considered important). In the health trust survey, integrity is ranked as the most important aspect, followed by availability and quality as the second and third most important. Confidentiality, although considered important, is ranked lowest of the four aspects. In the NPR case, the opposite was found with confidentiality score beeing the highest. A possible explanation can be as follows:
Health trusts are primary concerned with the life and health of the patient and prioritizing of integrity, quality and availability seems very sensible. From a treatment point of view, saving a patient's life is more important than the risk of unintentional disclosure of personal information, in other words - focus is on patient security. In contrast, the health registers are 'secondary users' of health information, and these are not directly involved in the treatment of the patient. They also possess very large amounts of personal data so the focus on confidentiality seems to be a right prioritization with the timely delivery of information beeing less critical here.

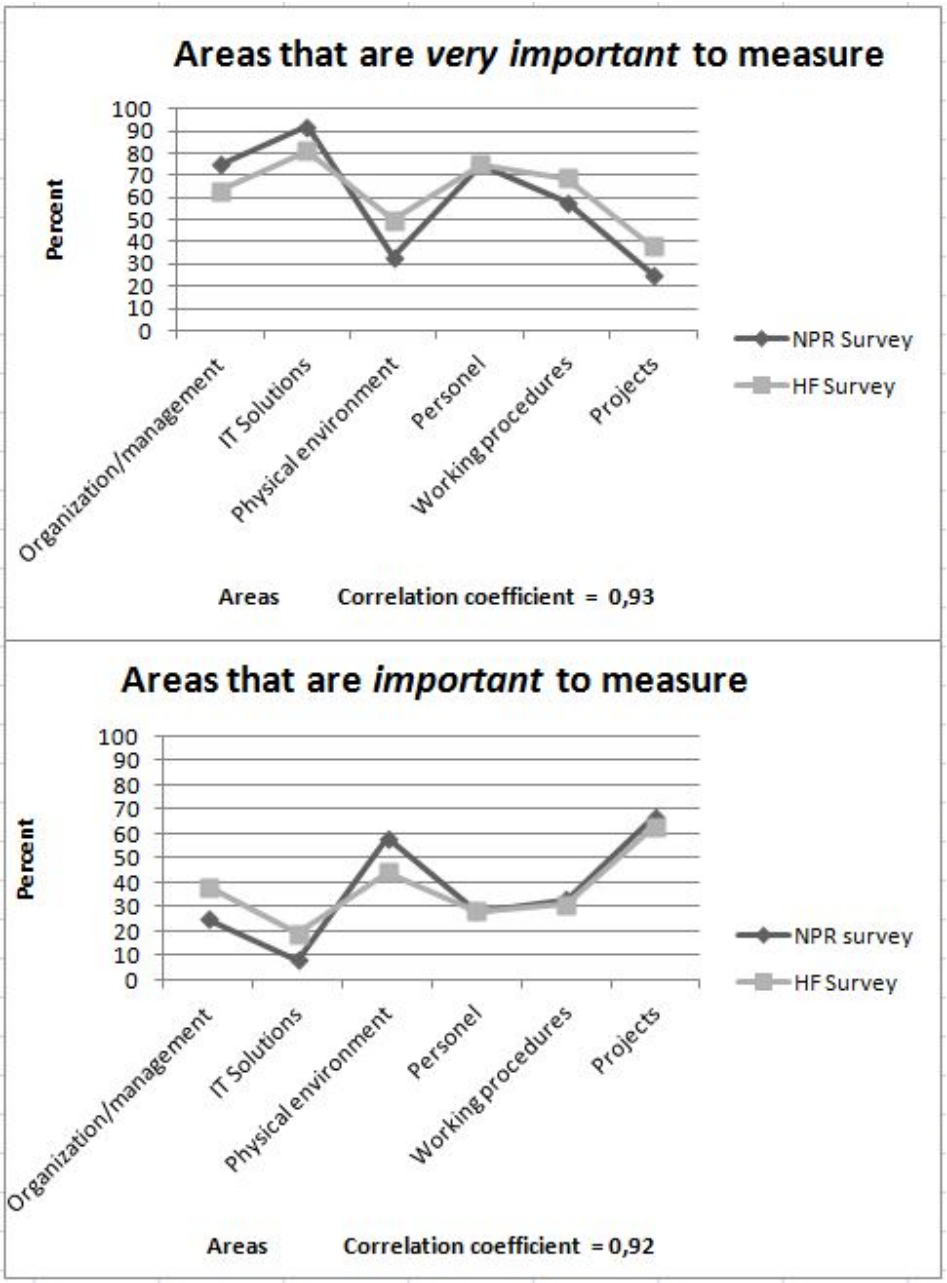

Figure 18: Correlation between important measurement areas - HF and NPR internal survey

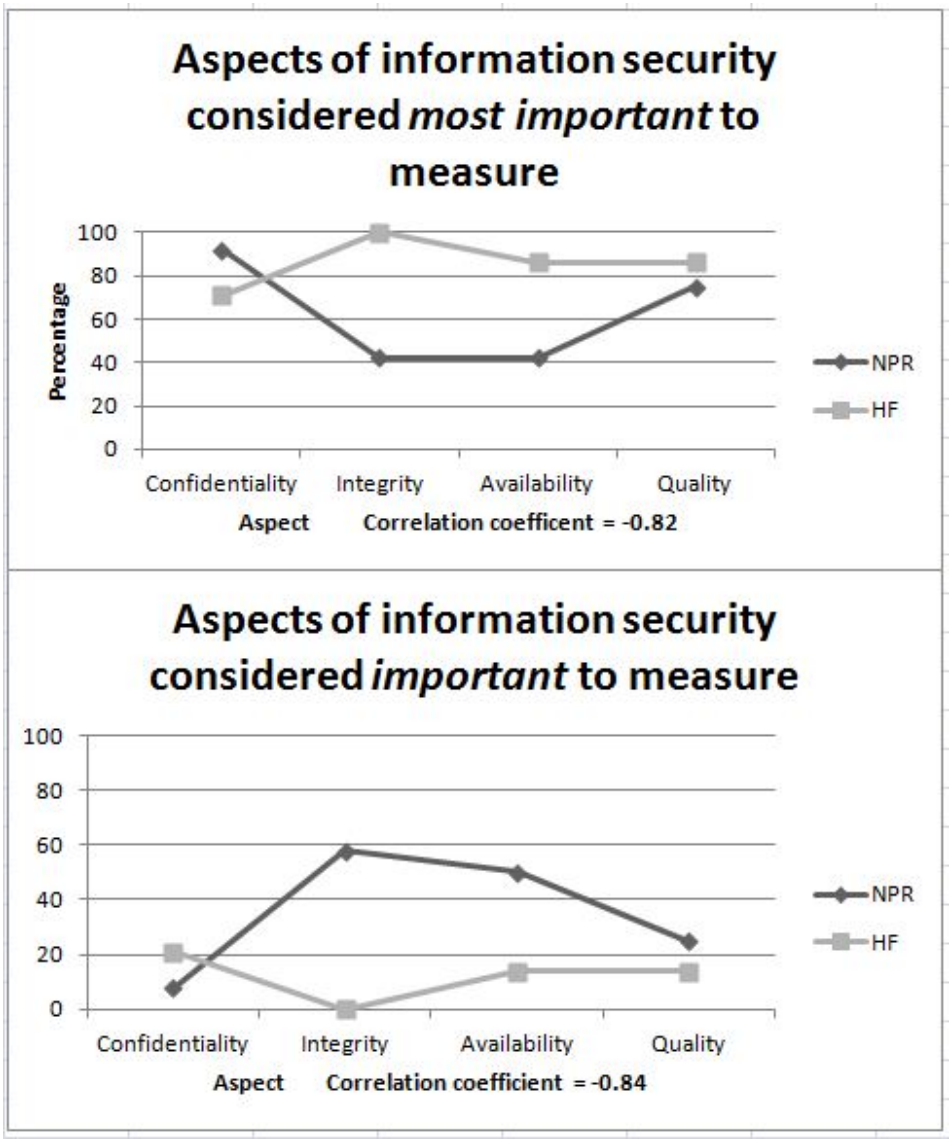

Figure 19: Correlation between important measurement aspects - HF and NPR internal survey

9 Future Work

The following areas for future work were identified from the case study and survey:

- Estimation of the value of the health information to be protected - it is hard to find the correct level for investment in information security (and measuements of such) in health care when the value of the information to protect is unknown. More knowledge on the cost of security breaches and its frequencies in health care could be prove helpful to establish this.
- What are the incentives behind security breaches in the health care sector? ('Know your Enemy') Counter stakeholders for information security exists and measures like proper legislation can prove helpful (E.g. is there an economic motivation for life-insurance agents to increase their salary based on illegal access to the insured persons medical information?)

Further research should also be done in order to gain knowledge on the information security in health research projects. (See also [60]).

10 Concluding Remarks

The study shows that the selected information security measurements in the case were worthwhile in terms of the benefits they provided compared with the costs of providing them. This is also in accordance with the opinions on security measurements from personnel working with information security in the Norwegian health trusts. The data from the NPR case study suggest that confidentiality is the most important aspect to measure in the Norwegian health registers.
The 'Code of Conduct for information security in the healthcare, care, and social services sector'[12] has a vital role in Norwegian healthcare and all respondents in the survey indicate that it is used as a basis for their Information Security Management System (ISMS). The majority of the respondents is of the opinion that 'the Code' also should encompass compulsory measurements of information security.
One obstacle of implementing information security measurements in the health care sector is that the benefits are hard to quantify in monetary values. The 'value' of the data they safeguard, or the cost of security breaches, are unknown and further research in this area will help establishing a correct level for information security measures, controls and measurements. It is also difficult to establish correct security level including measurements, when the actual threats to the systems are unknown. Thus, further research regarding the incentives behind security breaches in the health sector could prove helpful.

Bibliography

[1] Alsaker, M. Rapport 08/04 indikatorer for måling av informasjonssikkerhet. Technical report, Norwegian Centre for Informatics in Health and Social Care (KITH), Trondheim, Norway, 2004.

[2] Savola, R. Jan 2010. On the feasibility of utilizing security metrics in software-intensive systems. *IJCSNS International Journal of Computer Science and Network Security*, 10.

[3] Schneier, B. 2000. *Secret and lies: digital security in a networked world*. Wiley Computer Publishing, New York, NY USA.

[4] Grimson, J., Stephens, G., Jung, B., Grimson, W., Berry, D., & Pardon, S. June 2001. Sharing health-care records over the internet. *Internet Computing, IEEE*, 5(3), 49 –58.

[5] Norwegian Ministry of Health and Care Services. June 2009. Report no. 47 (2008-2009) to The Storting: The Coordination Reform.

[6] Shostack, A. & Stewart, A. 2008. *IT Security Metrics: The New School of Information Security*. Pearson Education, Inc, Boston, MA USA.

[7] Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. Nist 800-55 performance measurement guide for information security. Technical report, National Institute of Standards and Technology, Gaithersburg MD, USA, 2008.

[8] ISO/IEC. ISO/IEC: 27004:2009 Information technology - Security techniques - Information security management - Measurement. Technical report, International Organization for Standardization, Geneva, Switzerland., 2009.

[9] Savola, R. nov 2011. Security metrics for software systems -objectives and challenges. Presentation at COINS security metrics conference, Stockholm University.

[10] Jaquith, A. 2007. *Security Metrics: Replacing fear,uncertainty and doubt*. Pearson Education Inc.,Addison Wesley, Upper Saddle River, NJ USA.

[11] Vatnoy, T. 2007. *Medvirkning Samhandling Sikkerhet - IKT i helsetjenesten*. Conflux AS, Oslo, Norway.

[12] Norwegian Directorate of Health. September 2006. Code of conduct for information security in the healthcare, care, and social services sector. `http://www.helsedirektoratet.no/vp/multimedia/archive/00011/Faktaark_2_-_Styring_11347a.pdf` (Visited on 2010-12-21).

[13] Bakaas, T. H. God praksis for måling av informasjonssikkerhetsnivå. Master's thesis, GUC -Gjøvik University College, June 2005.

[14] Rose, A., Peters, B., Shea, J., & Armstrong, K. Jan 2004. Development and Testing of the Health Care System Distrust Scale. *JGIM, Journal of General Internal Medicine*, 19.

[15] Onabajo, A. & Jahnke, J. 0-0 2006. Properties of confidentiality requirements. In *Computer-Based Medical Systems, 2006. CBMS 2006. 19th IEEE International Symposium on*, 841 –846.

[16] Jussboka.no. Journalsnoking. `http://www.jussboka.no/2009/07/journalsnoking/`)Visited on 2011-11-26).

[17] U.S. Department of Health & Human Services. Breach notification rule - breaches affecting 500 or more individuals. `http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html`)Visited on 2011-11-26).

[18] SC Magazine. Us firm robbed of 4.2 million health records. `http://www.scmagazine.com.au/News/280442,us-firm-robbed-of-42-million-health-records.aspx`)Visited on 2011-11-26).

[19] Leedy, P. D. & Ormrod, J. E. 2005. *Practical Research, Planning and Design, 8th edition*. Pearson Education, Inc, Upper Saddle River, NJ USA.

[20] Wikipedia. nov 2011. Scientific modelling. `http://en.wikipedia.org/wiki/Scientific_model` (Visited on 2011-11-21).

[21] Hayden, L. 2010. *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*. McGraw-Hill, New York, NY USA.

[22] ISO/IEC. ISO/IEC: 15939:2007 Systems and software engineering – Measurement process. Technical report, International Organization for Standardization, Geneva, Switzerland., 2007.

[23] Kaplan, R. S. & Norton, D. P. 2004. *Strategy maps: converting intangible assets into tangible outcomes*. Harvard Business School Publishing, Boston, MA USA.

[24] Deming, W. E. 2000. *Out of the Crisis*. MIT-Press, Cambridge, MA USA.

[25] Barabanov, R. Information security metrics - state of the art - draft 0.7. Technical report, COINS project, Stockholm University, Sweden, November 2010.

[26] Bellovin, S. M. 2006. On the brittleness of software and the infeasibility of security metrics. *IEEE Security and Privacy*, 4(4), 96.

[27] McHugh, J. may 2002. Quantitative measures of assurance: Prophecy,process or pipedream? In *Proc. of Workshop on Information Security System Scoring and Ranking (WISSSR)*, ACSA and MITRE.

[28] Burris, P. & King, C. july 2001. A few good security metrics. http://www.metagroup.com/metaview/mv0314/mv0314.html/.

[29] Swanson, M., Bartol, N., Sabato, J., Hash, J., & Graffo, L. Security metrics guide for information technology systems. Technical report, National Institute of Standards and Technology, Gaithersburg MD, USA, 2003.

[30] ISO/IEC. ISO/IEC: 27001:2005 Information technology - Security techniques - Information security management systems - Requirements. Technical report, International Organization for Standardization, Geneva, Switzerland., 2005.

[31] ISO/IEC. ISO/IEC 15408-1:2009 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. Technical report, International Organization for Standardization, Geneva, Switzerland., 2009.

[32] Federal Information Processing Standards Publication. FIPS PUB 140-2, Security requirements for cryptographic modules. Technical report, National Institute of Standards and Technology, Gaithersburg MD, USA, 2002.

[33] ISACA. COBIT - Control Objectives for Information and related Technology. http://www.isaca.org)Visited on 2011-11-26).

[34] Forum, I. S. June 2011. Information security forum - tools and methodologies. https://www.securityforum.org/services/publictools/ (Visited on 2011-06-26).

[35] Turn, R. & Shapiro, N. Z. 1972. Privacy and security in databank systems: measures of effectiveness, costs, and protector-intruder interactions. In *Proceedings of the December 5-7, 1972, fall joint computer conference, part I*, AFIPS '72 (Fall, part I), 435–444, New York, NY, USA. ACM.

[36] Gordon, L. A. & Loeb, M. P. 2006. *Managing Cybersecurity Resources - A Cost benefit Analysis*. McGraw-Hill, New York, USA.

[37] Shostack, A. & Stewart, A. 2008. *The New School of Information Security*. Pearson Education, Inc, Boston, MA USA.

[38] Richardson, R. 2010 / 2011 CSI Computer Crime and Security Survey. Technical report, Computer Security Institute, jun 2011.

[39] Muennig, P. 2008. *Cost-Effectiveness Analysis in Health: A Practical Approach , Second edition*. Jossey-Bass, 989 Market Street, SF USA.

[40] Dahl, S. & others (editors). apr 2009. Norway and health. an introduction. (is-1703).

[41] Ministry of Health and Care Services. May 2001. Lov 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger. http://www.lovdata.no/all/hl-20010518-024.html (Visited on 2011-02-27).

[42] Audestad, J. A. Information society and security. Technical report, Gjovik University College, 2009. Compendium.

[43] Andresen, H. 2009. The policy debate on pseudonymous health registers in norway. In *Biomedical Engineering Systems and Technologies*, Fred, A., Filipe, J., & Gamboa, H., eds, volume 25 of *Communications in Computer and Information Science*, 413–424. Springer Berlin Heidelberg.

[44] Ørstavik R., Cappelen I., S. C. Helseregistre redder liv. Technical report, The Norwegian Institute of Public Health, May 2005.

[45] The Ministry of Health and Care Services. December 2007. For 2007-12-07 nr 1389: Forskrift om innsamling og behandling av helseopplysninger i norsk pasientregister. `http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20071207-1389.html` (Visited on 2011-02-21).

[46] Ministry of Labour and Government Administration. December 2000. Act of 14 april 2000 no. 31 relating to the processing of personal data (personal data act). `http://www.lovdata.no/all/hl-20000414-031.html` (Visited on 2011-02-27).

[47] Ministry of Labour and Government Administration. December 2000. For-2000-12-15-1265: Regulations on the processing of personal data. `http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001215-1265.html` (Visited on 2011-02-21).

[48] PMI. A guide to the project management body of knowledge. Technical report, Project Management Institute, December 2008.

[49] Boolsen, M. W. 2008. *Sporgeskemaundersokelser*. Hans Reitzels forlag, Copenhagen, Denmark.

[50] Savola, R. M. 2007. Towards a taxonomy for information security metrics. In *QoP '07: Proceedings of the 2007 ACM workshop on Quality of protection*, 28–30, New York, NY, USA. ACM.

[51] Ryan, J. & Ryan, D. sept.-oct. 2008. Performance metrics for information security risk management. *Security Privacy, IEEE*, 6(5), 38 –44.

[52] Ministry of Health and Care Services. June 2008. Lov 2008-06-20 nr 44: Lov om medisinsk og helsefaglig forskning (helseforskningsloven). `http://www.lovdata.no/all/hl-20080620-044.html` (Visited on 2011-02-27).

[53] Chen, T. november-december 2010. Stuxnet, the real start of cyber warfare? [editor's note]. *Network, IEEE*, 24(6), 2 –3.

[54] UK - Stationary Office. 2006. *ITIL V3 Foundation Handbook*. UK - Stationary Office, London, UK.

[55] Aftenbladet. Stadig flere pass forsvinner i posten. http://www.aftenbladet.no/innenriks/Stadig-flere-pass-forsvinner-i-posten-1832949.html)Visited on 2011-10-27).

[56] Quinn, S., Waltermire, D., & Johnson, C.and Scarfone, K. . B. J. The technical specification for the security content automation protocol. Technical report, National Institute of Standards and Technology, Gaithersburg MD, USA, 2009.

[57] Brenner, B. November 2008. Gary Hinson on ISO/IEC 27000. http://news.idg.no/cw/art.cfm?id=B6C47C6A-17A4-0F78-314CE240C89E43EF (Visited on 2010-12-21).

[58] Norwegian Directorate of Health. dec 2010. Is-1878 rammeverk for et kvalitetsindikatorsystem i helsetjenesten. http://www.helsedirektoratet.no/vp/multimedia/archive/00319/Rammeverk_for_kvali_319359a.pdf (Visited on 2011-06-27).

[59] Norwegian Directorate of Health. December 2010. Code of conduct for information security in the health sector - factsheet 2 isms rev. 2.1. http://www.helsedirektoratet.no/vp/multimedia/archive/00012/Summary_of_The_Code__12645a.pdf (Visited on 2011-06-21).

[60] Datatilsynet. Strategi for godt personvern i helsesektoren. http://www.datatilsynet.no/upload/Dokumenter/Strategi%20for%20et%20godt%20personvern%20i%20helsesektoren-17NOV2011.pdf)Visited on 2011-11-26).

[61] Barth Eide, Espen. Opening speech by Norwegian Defence Minister on a NSM security conference nov 17, 2011. http://www.regjeringen.no/nn/Subnettstader/europaportalen/nyheter-europaportalen.html?contentid=663562&id=449646)Visited on 2011-11-26).

[62] NORSIS - Norsk senter for informasjonssikring. Veiledning for outsourcing av IT. http://norsis.no/veiledninger/ledelse/Veiledning_outsourcing_IT.pdf)Visited on 2011-11-26).

[63] Wonnacott, R.J. Wonnacott, T.H. 1985. *Introductory Statistics - Fourth Edition*. John Wiley and Sons, New York, USA.

A List of Abbreviations

ALE - Annual Loss Expectancy
ATM - Automatic Teller Machine (minibank)
BCA - Benefit Cost Analysis
CBA - Cost Benefit Analysis
CEA - Cost Effectiveness Analysis
CMDB - Configuration Management Database
CMVP - Cryptographic Module Validation Program
COBIT - Control Objectives for Information and related Technology
EMR - Electronic Medical Record
EHR - Electronic Health Record
FIPS - Federal Information Processing Standard
FIRM - Fundamental Information Risk Management
HF - Norwegian Regional Health Trust (Helseforetak)
HOD - Norwegian Ministry of Health and Care Services (Helse og Omsorgsdepartementet)
ICT - Information and Communication Technology
IT - information Technology
ITIL - IT Infrastructure Library
ICD - The International Statistical Classification of Diseases and Related Health Problems maintained by WHO
IEC - International Electrotechnical Commission
IRR - Internal Revenue Rate
ISF - Information Security Forum
ISO - Internatinonal Organization for Standardization
ISMP - Information Security Measurement Program
ISMS - Information Security Management System
IS - Information Security
ISF - Norwegian healthcare Activity-based Financing (Innsatsstyrt Finansiering)
KITH - Center of Competence for IT in the Health and Social sector (Kompetansesenter for IT i helse- og sosialsektoren)
KPI - Key Performance Indicator
MRI - Magnetic Resonance Imaging
NCMP - Norwegian Classification of Medical Procedures
NCSP - The NOMESCO Classification of Surgical Procedures
NIPH - Norwegian Institute of Public Health (Folkehelseinstituttet - FHI)
NIST - National Institute of Standards and Technology (USA)
NPR - Norwegian Patient Registry
NPV - Net Present Value

PACS - Picture Archiving Control System
PDCA - Plan-Do-Check-Act
PID - Personal ID number
REK - Norwegian Regional Ethical Committee for Research - Regional Etisk Komite
RHF - Norwegian Regional Health Authority (Regionhelseforetak)
ROI - Return on Investment
ROSI - Return on Security Investment
SLA - Service Level Agreement
SSN - Social Security Number
TCO - Total Cost of Ownership
WHO - World Health Organization

B Listing of questions in the health trust web survey (in Norwegian)

Spørreundersøkelse - måling av informasjonssikkerhet i helseforetak (HF) / øvrige virksomheter

En Victorinox USB Flash lommekniv trekkes ut blandt deltagerne i spørreundersøkelsen.

-Et hendig verktøy med 2GB minnekapasitet.

Måling av informasjonsssikkerhet søker å finne ut om en organisasjon beveger seg i riktig retning med hensyn til konfidensialitet, integritet og tilgjenglighet på informasjon.

Etterlevelse av krav til informasjonssikkerhet samt å følge med på utvikling i omfang og typer av sikkerhetshendelser/-brudd er områder som det også anses som viktig å følge med på.

Resultatet av slike målinger vil så kunne gi nyttig informasjon om sikkerhetstiltak har den ønskede effekt.

Det er ikke stilt krav om slike målinger i Norm for informasjonssikkerhet i helse- omsorgs- og sosialsektoren ("Normen") og det er uvisst i hvilken grad de ulike aktørene gjør dette.
Undersøkelsen søker å avdekke i hvilken grad målinger gjøres, og hvilke holdninger de enkelte aktører har til dette.

Resultatene fra denne undersøkelsen vil gjøre det mulig for de enkelte helseforetak (HF) å sammenligne seg med hva andre helseforetak av tilsvarende størrelse gjør . Undersøkelsen er delvis anonym, det vil si at institusjoner ikke navngis men det spørres om tilhørighet til RHF og størrelse på foretaket i undersøkelsen.

Resultatene fra denne undersøkelsen vil bli publisert på Høgskolen i Gjøvik sine hjemmesider www.hig.no forutsatt at oppgaven tilfredstiller skolens kriterier.

Hjelp >>

Bakgrunnsinformasjon

Denne delen av undersøkelsen henter inn litt bakgrunnsinformasjon for besvarelsen

1. Er du mann / kvinne?

- Mann
- Kvinne

2. Hvor gammel er du?

- 29 år eller yngre
- 30 - 39 år
- 40 - 49 år
- 50 - 59 år
- 60 år eller eldre

3. Hvilket regionalt helseforetak (RHF) evt. annen kategori hører din organisasjon hjemme i?

- Helse Nord
- Helse Midt-Norge
- Helse Vest
- Helse Sør-Øst
- Annet/statlig
- Annet/privat

4. Hvor mange ansatte er det i helseforetaket eller virksomheten du tilhører? (angi ca. tall - helst antall ansatte da dette som regel er en del større enn antall årsverk.)

- Stort helseforetak/organisasjon (> 5000 ansatte)
- Middels stort helseforetak/organisasjon (2000 - 5000 ansatte)
- Mindre helseforetak/organisasjon (200 - 2000 ansatte)
- Lite helseforetak/ organisasjon (< 200 ansatte)

5. Hvor stor del av stillingen din er satt av til arbeid med informasjonssikkerhet i virksomheten?

- Full tid (100%)
- Deltid (20 - 99%)
- Mindre del av stilling (5 -20%)
- Jobber ikke til daglig med informasjonssikkerhet (mindre enn 5%)

6. Hvor mange er det totalt sett i virksomheten som er jobber heltid (dedikert) med informasjonssikkerhet?

- Ingen
- 1 person
- 2-5 personer
- 6 eller flere personer
- Vet ikke

<< Start på nytt Hjelp >>

7. Er det satt mål for informasjonssikkerhet i virksomheten?
(Med mål menes en vedtatt 'Policy for informasjonssikkerhet' eller annet styrende dokument som overordnet beskriver målsetting)

- Ja
- Nei
- Vet ikke

8. Gjøres det målinger av informasjonssikkerhet i virksomheten?

- Ja
- Nei
- Vet ikke

<< Start på nytt Hjelp >>

9. I hvilken grad er du kjent med følgende dokumenter/ standarder for måling av informasjonssikkerhet?
Angi på en skala fra 1 til 4 hvor
1 - meget godt kjent med
2 - kjenner til
3 - noe kjennskap til
4 - har ikke kjennskap til

	1	2	3	4
KITH rapport - indikatorer for måling av informasjonssikkerhet (KITH R08/04)				
Information Security Forums (ISF) Benchmark 2009 (tidligere ISF Security Status Survey)				
Information Security Forums (ISF) FIRM				
NIST SP 800-55 (National Institute of Standards and Technologies - US dept. of Commerce)				
ISO/IEC 27004 -2009				

10. I hvilken grad er du enig /uenig i følgende påstander - angi på en skala fra 1 til 4 hvor

1 er Helt Enig
4 er Helt Uenig

	1	2	3	4
Det er viktig å følge med på hvordan informasjonssikkerhet utvikler seg over tid	○	○	○	○
Målinger av informasjonssikkerhet bør inngå i foretakets SLA (Service Level Agreement) avtaler	○	○	○	○
Målinger av informasjonssikkerhet bør inngå i rapportering sammen med foretakets øvrige kvalitetsindikatorer	○	○	○	○
Status for informasjonssikkerhetsarbeidet rapporteres jevnlig til ledelsen	○	○	○	○
ISO standarder er vanskelig å forstå / implementere	○	○	○	○
Det er kostbart å måle informasjonssikkerhet (kost større enn nytte)	○	○	○	○
Målinger av informasjonssikkerhet etterspørres av ledelsen	○	○	○	○
"Normen" burde omfatte noen obligatoriske målinger av informasjonssikkerhet	○	○	○	○
Måling av informasjonssikkerhet er lite hensiktsmessig	○	○	○	○

<< Start på nytt Hjelp >>

11. Har status for informasjonssikkerhet i foretaket vært gjennomgått av ledergruppe i 2010?

Ja	○
Nei	○
Vet ikke	○

<< Start på nytt Hjelp >>

12. Hvilken dato ble dette gjennomgått? (spørsmålet kan hoppes over hvis dato er ukjent)

13. Hvilke områder har vært tema for en slik gjennomgang?

	Ja	Nei	Vet ikke
Styringsystem for informasjonssikkerhet (ISMS)	○	○	○
Rapporterte avvik /sikkerhetshendelser	○	○	○
Gjennomføring av risikovurderinger	○	○	○
Tiltak for å bedre informasjonssikkerhet	○	○	○
Opplæring av ansatte	○	○	○
Sikkerhetsrevisjoner	○	○	○

<< Start på nytt Hjelp >>

14. Hvilke(n) standard(er) benyttes i styringssystemet for informasjonssikkerhet?

(Flere valg er mulig her)

- ☐ Eget styringssystem
- ☐ Basert på Norm for informasjonssikkerhet
- ☐ ISO/IEC 27002
- ☐ ISO/IEC 27001
- ☐ ITIL (IT Infrastructure Library)
- ☐ COBIT (Control Objectives for Information and related Technology)
- ☐ Annen standard

<< Start på nytt Hjelp >>

15. Omfatter styringssystemet for informasjonssikkerhet også forskningsprosjekter i organisasjonen?

- Ja, dette omfattes og ivaretas av styringssystemet
- Nei, informasjonssikkerhet i de enkelte forskningsprosjekter er prosjektleders ansvar
- Nei, men styringssystemet vil etterhvert utvides til å omfatte dette.
- Vet ikke
- Ikke relevant
- Annet / kommentar

<< Start på nytt Hjelp >>

16. Hvilke egenskaper ved informasjonssikkerhet tror du det er viktigst å følge med på?
Angi på en skala fra 1 - 4 der
1 er Svært viktig
2 er Viktig
3 er Mindre viktig
4 er Ikke viktig

	1	2	3	4
Konfidensialitet (Informasjon er tilgjenglig kun for de som har tjenestlig behov)				
Integritet (At informasjon er sikret mot utilsiktet eller uautorisert endring)				
Tilgjenglighet (At informasjonen er tilgjenglig når den etterspørres)				
Kvalitet (At det er rett informasjon som ligger i systemet)				

<< Start på nytt Hjelp >>

17. Angi hvor viktig du mener det er å måle informasjonssikkerhet i områdene angitt under?
(eksempler innenfor hvert område er angitt i parantes)
1 er Svært viktig
2 er Viktig
3 er Mindre viktig
4 er Ikke viktig

	1	2	3	4
Organisasjon/ledelse (etterlevelse av regelverk, vurdere risko , måle avvik, tildele autorisasjoner, korrigerende tiltak)	○	○	○	○
IT løsninger (konfigurasjon, endring, sikkerhetstiltak,brannmur, antivirus etc.)	○	○	○	○
Fysisk miljø (adgangskontroll, låser, skap, brannsikring, strøm etc.)	○	○	○	○
Personell (opplæring i informasjonssikkerhet, holdninger)	○	○	○	○
Arbeidsprosedyrer	○	○	○	○
Prosjekter (ivaretakelse av informasjonssikkerhet i disse)	○	○	○	○

Andre områder (legg gjerne inn forslag i fritekst felt)

<< Start på nytt Hjelp >>

Takk for deltagelsen!

For å delta i trekningen av en Victorinox lommekniv, så send en e-post med emne 'Lommekniv' til sjur.hartveit@hig.no.

Trekningen av vinner vil bli foretatt 1. oktober

Med vennlig hilsen
Sjur Hartveit
Masterstudent
Høgskolen i Gjøvik.

<< Start på nytt Hjelp Avslutt