Security Incident handling and reporting

a study of the difference between theory and practice

Tore Larsen Orderløkken

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2005

The MSc programme in Information Security is run in cooperation with the Royal Institute of Technology (KTH) in Stockholm.

Institutt 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

Table of contents

Tables

Figures

Abstract

Increasingly private companies and public institutions are more dependent on reliable and secure Information and Communication Technology (ICT) solutions. The increase in business to business and business to consumer handling has forced an increased level of availability against the organisation's ICT systems. In addition, the fast growth in the number of Internet users, increased broadband and increased ICT expertise at the users (also knowledge about how security mechanisms are breached) present considerable challenges related to maintaining security in the solutions that are available on the Internet. This also applies to a great extent to the organisation's internal network. With a background as complex as this, security incidents occur from time to time. These are incidents, which in one way or another exploit weaknesses in systems, services or programs so that this causes a breach either of confidentiality, availability or integrity. Through literature, media, ICT and security education many theoretical approaches have emerged for how to handle such security incidents and how to report them. However, very little is known about what happens in practice and how efficiently companies and institutions see to their security incidents. It is also uncertain how different companies and institutions define what constitutes a security incident. So how do different organisations handle a security incident?

- Are security routines defined so that one knows when an incident has occurred?
- Are there routines for how a security incident shall be handled?
- Are there reporting routines that function so that those seeing to security incidents are notified?
- Is there a difference in how public institutions and private companies handle security incidents?

We have conducted a survey of Norwegian companies and public institutions to find answers to these questions. Security managers and others working with security have responded to a survey concerning these matters.

To be able to give correct answers on the level of handling security incidents, we have also developed security metrics that can be used to verify this. These metrics can be used internally or as measuring points towards suppliers, contractors, third party or outsourcing vendors.

Through the answers from the survey, we see a difference in how public and private organisations handle their security incidents. The public organisations have shortcomings in the way they handle security incidents such as policy level, training and practice, compared to how private organisations handle their security incidents. If we look at the organisations gathered, we can also find room for improvements in the private domain, especially connected to reporting, training and statistics regarding the number of reported security incidents.

Sammendrag (Abstract in Norwegian).

Private bedrifter og offentlige institusjoner er i stadig sterkere grad avhengig av pålitelige og sikre Informasjon og Kommunikasjons Teknologi (IKT) løsninger. Økning i ”business to business” samt ”business to consumer” fremtvinger en økt tilgjengelighet inn mot organisasjonenes IKT systemer. En rask vekst i antall brukere på Internett, økt båndbredde og økt IKT kompetanse hos brukerne (også kunnskap om hvordan de bryter sikkerhetsmekanismer) gir større utfordringer knyttet til å ivareta sikkerheten i løsningene som tilgjengliggjøres på Internett. Dette gjelder i høyeste grad i organisasjonenes interne nett. I denne komplekse settingen vil det fra tid til annen oppstå sikkerhetshendelser. Dette er hendelser som på en eller annen måte utnytter svakheter i systemer, tjenester eller programmer slik at det medfører brudd på enten konfidensialitet, integritet eller tilgjengelighet. Det er gjennom litteratur, medieoppslag og i forskjellige IKT og sikkerhetsutdanninger mange teoretiske tilnærminger til hvordan man skal håndtere slike sikkerhetshendelser og rapportere disse. Imidlertid er det lite kjent hvordan dette skjer i praksis og hvor effektivt bedrifter og institusjoner ivaretar sine sikkerhetshendelser. Det er også uvisst hvordan forskjellige bedrifter og offentlige institusjoner definerer hva som er en sikkerhetshendelse. Hvordan håndterer så de forskjellige organisasjoner en sikkerhetshendelse?

- Er sikkerhetshendelser definert slik at man vet når de har inntruffet?
- Er det rutiner for hvordan en sikkerhetshendelse skal håndteres?
- Er det rapporteringsrutiner som fungerer slik at de som skal ivareta sikkerhetshendelsen blir varslet?
- Er det forskjell på hvordan offentlig institusjoner og private bedrifter håndterer sikkerhetshendelser.

Vi har gjort en undersøkelse blant norske bedrifter og offentlige institusjoner for å finne svarene på disse spørsmålene. Sikkerhetsledere og andre som jobber med sikkerhet har svart på et spørreskjema som berører disse temaene.
For å kunne gi svar på om man har håndteringsmekanismer på plass har vi også utviklet sikkerhetsmetrikker som kan brukes for å verifisere dette. Slike metrikker kan brukes internt som oppfølgingsverktøy eller som målepunkter mot outsourcingsleverandører og tredjeparter.

Gjennom svarene i spørreundersøkelsen ser vi en klar forskjell på hvordan offentlige og private organisasjoner håndterer sikkerhetshendelser. De offentlige organisasjonene har større mangler på sin hendelseshåndtering når det gjelder policynivå, opplæring og praksis i forhold til hvordan sikkerhetshendelser håndteres i private organisasjoner. Ser vi samlet på organisasjonene er det også for de private organisasjoner rom for forbedringer, spesielt knyttet til rapportering, opplæring og statistikk knyttet til hvor mange hendelser som blir rapportert.

Preface

This master thesis is the last part of the requirement to fulfill my master degree in information security at Gjøvik University College. The work with this thesis started 1st of January and ended 30th of June 2005.

I have been a part time student at Gjøvik University College, starting fall 2002. I have during this period had a full time position as manager of Center of Excellence Information Security in Telenor.

The work within the information security area in the past 10 years has given me a good understanding of the practical handling of information security in different organisations. One of my observations has been that in many cases security incidents are not very well taken care of.

This Master thesis is therefore a way of finding answers to my observations and trying to find ways to understand how security incidents can be effectively handled and reported.

During my work with the thesis project plan [31] I discovered that many theoretical approaches have been developed in this matter. However my impression was that there were challenges to get this theory implemented in real life organisations.

The work with this master thesis has taught me a great deal about how different organisations handle security incidents. This is knowledge I will use in my job in the future within the information security area.

Lillehammer 22nd of June 2005.

____

Tore Larsen Orderløkken

Acknowledgement

Thanks to Professor Slobodan Petrovic´ for guidance and feedback during the work.

Thanks to all who responded to the survey by giving answers to my questions.

Thanks to my employer Telenor for letting me fulfil this three years of study.

Thanks to my colleagues for giving me support.

Thanks to Jan Erik and Tone for support and help during my master education

Thanks to Inger, Mia Kamilla, Magnus and Sander for having patience with me during this 3 years period.

Audience

This Master thesis focuses on managing security incidents and is of main interest for personnel dealing with security organisation, security management and security policies.

Abbreviations/Definitions

CIRT	-	Computer Incident Response Team
CSIRT	-	Computer Security Incident Response team
CERT	-	Computer Emergency Response Team
Event		"A thing that happens or takes place, especially one of importance" [33].
IDS	-	Intrusion Detection System
Incident	-	"Something unusual, serious, or violent that happens" [34]. "A group of attacks that can be distinguished from other attacks because of the attackers, attacks, objectives, sites and timing" [2]. "A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices" [16].
Incident Handling:	-	"The mitigation of violations of security policies and recommended practices" [16].
Security Incident	-	"Any adverse event whereby some aspect of computer security could be threatened: Loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability" [16]

1 Introduction

1.1 Topic

To an increasing extent, communication between people takes place electronically, and more and more communication between machines and between people is affecting commerce, banks and finance and critical infrastructures such as electric power industry, oil industry and telecommunication industry. In this environment, security incidents resulting breaches of confidentiality, integrity or availability (CIA) from time to time occur. Such incidents can be deliberate internal or external actions, but they can also be unconscious actions by the same persons. Errors in applications, services and systems can also cause security incidents. When security incidents occur, there is considerable cause for concern if there are no routines or practices for how such incidents will be handled or reported.

In this Master Thesis we attempt to find out whether theory for such handling concurs with practice in different organisations. At the same time, we seek to find out how the public and private sector handle their security incidents and security incident reporting.

1.2 Key words

Technology, Management Science, Information Security, Security Incidents, Intrusion Detection Systems, Computer Incident Response Team, Incident Response, Security Incident Reporting, Security Incident handling, Security Incident Management, Computer Emergency Response Team, IDS, CIRT, CSIRT, CERT, Security Incidents, Security Incident Handling.

1.3 Problem description

There are descriptions of theories that indicate how to carry out security incident handling and security incident reporting. We are unsure whether these theories are effective or carried out in practice. In many cases top management does not know what a security incident is or how much damage or what type of damage a security incident causes or might cause. Proper handling and reporting of security incidents enables management to make decisions regarding the security level and security investments based on a correct threat evaluation. Another problem for the organisations is in what way do they measure their level of handling security incidents. Today's organisations more and more often outsource their IT systems. The follow up of Information security is then in most cases more difficult. We often wonder if our outsourcing partner handles security incidents according to agreed level. We shall in this master thesis find out if theory agrees with practice regarding security incident handling and if there is a difference in how public institutions and private companies handle security incidents. The problem associated with measuring how effective security incident handling is, will also be covered.

1.4 Motivation and justification

Security measures in an organisation are often implemented without management being aware of the threat situation or which security incidents one has been subject to or exposed to. A planned, practiced and functional routine for security incident handling and reporting contributes to the organisation saving money on security investments as well as losses. By defining the incident, and having routines for handling and reporting the incidents the organisations can have a profile of being a security conscious organisation. While at the same time by being familiar with the threat situation one can be proactive in security work. The dividends will be great and proper security incident handling can prevent a security incident from having serious consequences. Having good handling routines and procedures for security incidents also increases the employees´ involvement and the organisations will get more accurate figures over their security incidents. This again leads to improvements in security measures and turning organisations more proactive.

Interested parties (Stakeholders) in such a problem will typically be management, shareholders, chief administrative officers in local governments and provinces as well as those responsible for security in the organisation.

1.5 Research questions

In order to be able to underpin an assertion that even if the theoretical foundation exists, organisations do not carry out sufficient security incident handling and security incident reporting, it is important to obtain responses to research questions that indicate something about the situation in the individual organisations. As we have chosen to approach private and public organisations, it is important to ascertain whether there really is a difference between how these two branches handle and report their security incidents. Our hypotheses can be described as follows:

- Even if the theoretical foundation is in place, organisations does not handle security incidents according to the theory.
- There is a difference between how private and public organisations handle security incidents.

These hypotheses lead to the following research questions, which we attempt to answer in this master thesis:

1. Do organisations have routines for incident handling and reporting?
2. How do organisations define a security incident?
3. Are the organisations capable of discovering security incidents?

4. Is there any correlation between handling routines and reporting with respect to the degree and effect between public and private organisations?
5. Has the extent of introduction of security incident handling routines and training had any effect on the number of reported security incidents?
6. Is it possible to measure how effective security incident handling is?

2 Previous work

Handling security incidents and reporting them are described in many contexts and there are standards, guidelines, checklists, routines and procedures made available [17]. In most sources there is a theoretical approach to how to develop and implement security incident handling. The threat situation is constantly developing and increasingly, security incidents cause more damage when they occur. This chapter contains an overview of literature regarding what has been done in terms of the content of this master thesis and compared to the research questions in this report (Section 1.5).

2.1 Security incidents

An incident is defined in Oxford dictionary [33] as "An event or occurrence, especially a minor one". In Longman [34] an incident is referred to as "an event, especially one that is unusual, important or violent". To get a security incident one needs a violation of security. The literature has also different definitions of security incidents: "A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices" [16]. Another definition for security incident is "any event that may threaten or compromise the security, operation or integrity of computing resources" [6]. One problem, however, is to narrow down the definition of security incident. If we take all in consideration, a security incident could have implications on physical, logical or organisational matters. If we look into the "Internet Security Glossary" [35] the definition of security incident is "A security event that involves a security violation". Most of the literature studied during the work with this master thesis, discuss IT-Security incidents. These are security incidents that occur in the IT domain and are referred to as IT-Security incidents.

To find out more about what a security incident is, we have studied different literature sources. Understanding what constitutes a security incident will be very important in the continuing work with this master thesis. Sandia National Laboratories have presented a taxonomy report entitled "A Common Language for Computer Security Incidents" [2]. The report gives a description on how to define security incidents using taxonomy. The report presents first a list of 24 different security incidents as a list of single, defined terms as shown in Figure 1.

Wiretapping
Dumpster diving
Eavesdropping on
Emanations
Denial-of-service
Harassment
Masquerading

Unauthorized data
copying
Degradation of service
Traffic analysis
Trap doors
Covert channels
Viruses and worms

Tunneling
Trojan horses
IP spoofing
Logic bombs
Session hijacking
Timing attacks

Data diddling
Salamis
Password sniffing
Excess privileges
scanning
Software piracy

Figure 1 List of single, defined terms [2].

The report then describes how this way of putting security incidents in categories does not give a correct description, because different incidents can have different elements. For instance a virus can contain a logical bomb. The Sandia report gives examples on how attackers use tools and vulnerabilities to take action against targets and how all these actions can be incidents. In this report, the accepted definition of incident is "- a group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing". This can be shown in Figure 2, which explains how and where security incidents occur.

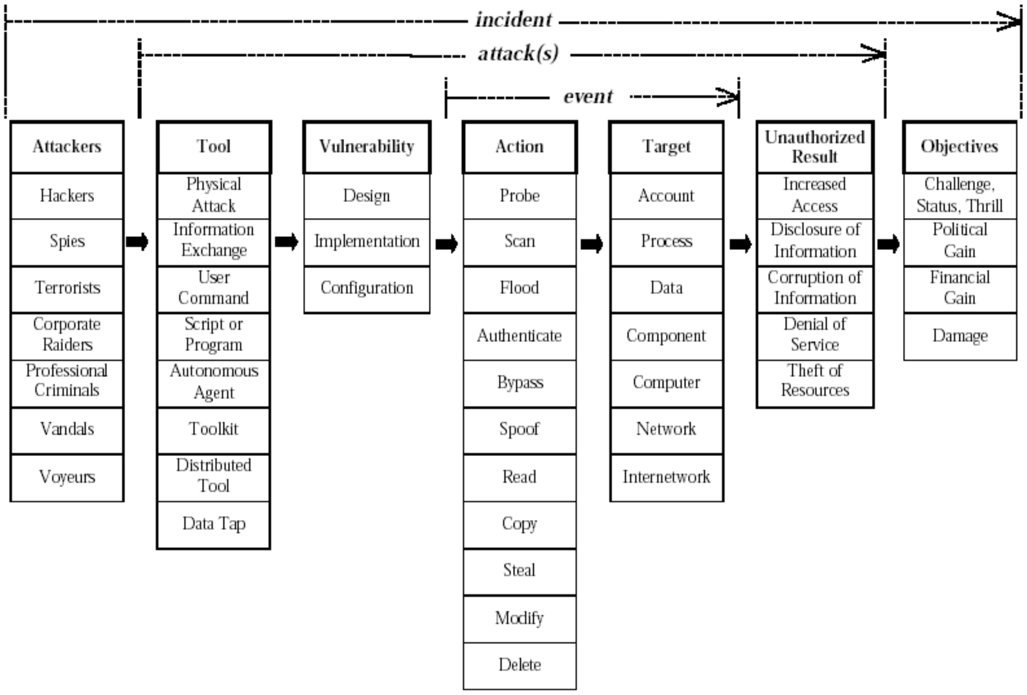


Figure 2 Where do incidents occur [2]

Others have also seen that a collection of documents related to security incident handling was missing. For this reason, they have gathered documentation related to security incident handling and an overview of definitions and different publications and websites on a dedicated website [17].

Security incidents can be triggered in many ways. Some examples are given in [36]:

- User errors
- Security loopholes in hardware or software components
- Computer viruses
- Disclosure of confidential data
- Loss of personnel resources
- Criminal action

2.2 Handling security incidents

To handle security incidents, one needs measures to respond to suspected or known breaches to security mechanisms or breaches to security safeguards. This response refers to routines, procedures, practices, technologies, services and/or human behaviour. One can also refer Incident handling to the mitigation of violations of security policies and recommended practices [16].

BS ISO/IEC 17799 [12, 13] provides general indications on how to handle security incidents. The standard gives general recommendations but no specific handling procedures or routines. This standard has become one of the leading standards towards the information security area, and BS7799 part 2 is the standard to be certified against. This implies that to be certified one needs security incident handling routines in place.

The Federal Office for Information security (BSI) has in their IT Baseline Protection Manual (IT BPM) [36] a description on how to handle security incidents. The manual describes the steps to accomplish a good handling of security incidents. The most important here is to have developed and practice a security incident policy. BSI states that it is not trivial to implement a security incident handling policy.

In January 2004, NIST published a guide [16] to security incident handling. This guide describes:

- Organisation of security incident handling capacity
- Establishment of policies and procedures
- Structuring an incident response team including outsourcing problems
- Who to include in incident handling
- Handling of incidents from preparatory work to follow up after an incident

In addition, different types of incidents are described as well as the handling of these incidents:

- Denial of Service (DoS)
- Malicious Code
- Unauthorized Access
- Inappropriate Usage
- Multiple Component.

The report describes in detail how organisations can organise their incident handling capacity and also gives some examples of different incidents and how to handle them. The basis for security incident handling according to this report is:

- Establish a formal incident response capability.
- Create an incident response policy and use it as the basis for incident response procedures.
- Establish policies and procedures regarding incident-related information sharing.
- Provide pertinent information on incidents to the appropriate incident-reporting organisation.

Thomas A Longstaff describes in [9] six principal areas within incident handling: "communications, intruder topics, malicious code, audit, procedures, and usability issues". Within each area, individual topics have been ranked and categorized by applicable time-scale. Longstaff focuses on which activities require further research. Sixteen different research suggestions are listed in the paper. The report concludes that further work should be carried out in creating tools to detect security incidents.

2.3 Reporting security incidents

Many organisations have routines for reporting security incidents. The implementation and training is however not as good. For this reason the statistical data over such incidents are deficient. Some organisations have tried to construct these figures, but they are sceptical about the figures because of under-reporting [4]. There are still many who do not report security incidents due to fear of damaging their reputations [5]. A survey carried out in cooperation between CSO magazine, the United States Secret Service and Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center (2004 e-crime watch survey) [5] shows a significant increase in the number of security incidents and e-crime estimates in 2003. Figures from the CERT Coordination Centre for 1988 - 2003 indicate the same trend [8].

In the 2004 E-Crime Watch Survey [5] regarding monitoring and reporting, 80% of respondents report that they monitor their computer systems or networks for misuse and abuse by employees or contractors. 95% of respondents say they use some type of employee monitoring (e.g., internet, email, files) to deter e-crime. 36% report using employee monitoring to terminate an employee or contractor, for illegal activities. 72% of respondents require internal reporting of misuse or abuse of computer access by employees or contractors. However, just under half (49%) of respondents say intrusions are handled with the help of law enforcement or by taking other legal action.

2.4 Incident Response Team

Another common finding in the literature when studying the handling of security incidents is a function called Computer Security Incident Response Team (CSIRT) [11, 15]. To handle IT-security incidents, almost all articles, reports and other literature advice to set up a CSIRT or a similar team. This team is: A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability) [16].

There are different approaches to setting up such teams but all indicate that by setting up CSIRT or similar team the organisations can handle security incidents in a better way. In [6] Richard L. Rollason-Reese gives a description of how security incidents can be dealt with by using an IRT unit (Incident Response Team).

The literature studies indicate that the most described resource against security incidents is the one where one can exploit the Incident Response Team proactively or in an emergency situations [7]. In [7] John P. Wack describes how one can build up a Computer Security Incident Response Capability (CSIRC) and how this can be used for dealing with security incidents.

When setting up a CSIRT, there are different factors that have to be considered in order to get the best possible result [16]:

- Consider the relevant factors when selecting an appropriate incident response team model.
- Select people with appropriate skills for the incident response team.
- Identify other groups within the organisation that may need to participate in incident handling.
- Determine which services the team should offer.

2.5 Relevant Norwegian publications

In Norway there are also a number of organisations that have published articles, reports and studies concerning security incident handling. Some examples are the following: Uninett Cert has prepared a description of such handling [1]. The report documents step-by-step which elements must be included in incident handling. The elements include:

- preparations/planning
- identifying the problem
- damage limitation
- cleaning up
- restoration and lessons learned.

Ernst and Young [3] describe an architecture for handling security incidents where elements such as:

- improvement
- detection
- limitation
- clearing and restoration

are important concepts.

2.6 Tools and methods

Literature indicates that most tools made for IT-security incident detecting are tools known as Intrusion Detection Systems (IDS) and Firewalls. In different ways these tools detect intrusion attempts or illegal traffic through firewalls in the organisation's network and report these to given persons on different types of consoles. The IDS systems retrieve information from sensors, firewall logs and other relevant log files. Here, skilled persons with knowledge of the IDS system carry out measures, either using CSIRT activities or just reporting to security managers or systems owners [10]. Other tools that are described in the literature are [36]:

- Alarm annunciation devices
- Remote indication of malfunctions
- Virus scanning programs
- Cryptographic checksums using encryption, checksums or digital signatures.

We have also studied different tools and methods dealing with project management and risk analysis to see if those had any elements of security incident handling [18-21]. Interestingly enough, we found that those tools and methods did not mention security incident handling.

2.7 Verification of the theory

We have not found many actual measurements of how all these theories describing security incident handling and reporting work in practice. In national and international literature searches we have found theory-based conclusions but few that refer to surveys or research on how an individual organisation carries out security incident handling in practice. There is also a lack of documentation on how this handling affects security levels and how one can give reliable information to stakeholders as to how a good security incident handling and reporting implementation can affect the business. In the 2004 e-crime watch survey [5] some aspects has been covered. E.g. a question like:

Does your organisation monitor its computer systems and networks for misuse or abuse by employees or contractors? (Base: 500).

The statistical data from this survey show that the majority do monitor their computer systems and networks for misuse or abuse.

Yes	80.4%
Yes, systems only	4.8%
Yes, networks only	8.4%
Yes, both	67.2%
No	13.4%
Don't know	6.2%

Table 1 Monitoring.

Does your organisation require internal reporting of misuse or abuse of computer access by employees or contractors? (Base: 500).

The survey here indicates that some organisations have not implemented good routines when it comes to reporting incidents.

Yes	71.8%
No	18.0%
Don't know	10.2%

Table 2 Reporting incidents.

3 Choice of methodology

The main focus in this thesis is to see how private and public organisations handle security incidents and report them. This thesis is practical in its approach, and underpins the hypothesis that there is a difference in how the theory describes security incident handling and reporting and how this actually functions in the individual organisations. Through this thesis, we hope to direct focus on how reflected, actual handling and reporting can increase security and security consciousness in an organisation. In order to do this, in this master thesis we use the following methodology:

- Study of relevant literature
- Survey among selected Norwegian private and public organisations
- Prepare a draft version of a checklist for security incident handling and reporting
- Make security metrics to measure effect and implementation of security incident handling.

As a basis for carrying out the survey, we use lecture notes and foils from "Vitenskapelige metoder" (Scientific Methods [24]) as well as definitions from John W. Creswell's book [32]. The focus for this master will be on research questions in Section 1.5 and to find appropriate methods to acquire the knowledge and experience possessed by different organisations.

3.1 Study of relevant literature

The study of relevant literature mainly consists of books, articles, lectures, publications and similar, which contain facts related to the topic of this thesis. Through different types of searches that we learned in "Vitenskapelige metoder" (Scientific Methods [24]) we shall find relevant material that can be used in the Previous work chapter (2) and as a foundation for research questions in the master thesis. Studying the relevant literature is appropriate as the subject of security incident handling and reporting is well documented by many authors and professionals. For this reason, the study of relevant literature is appropriate in terms of being able to contribute to the theoretical foundation of the thesis. In spite of a large body of material, we have found very little that describes how different organisations carry out this handling in practice and how effective it is.

The literature study consist of specified searches on the Internet, searches in known scientific databases both through membership at Gjøvik University College and in open databases. We have used for example:

- IEEEXplore
- CiteSeer
- ISI - Web of science

- SpringerLink
- Google
- ACM – The guide to Computing Litterature
- Scirus – for scientific information only
- Bibsys – Gjøvik University College library system

3.2 Survey

In this master thesis a survey has been carried out to get an overview of how Norwegian private and public organisations handle their security incidents. Here it is the most relevant to use a quantitative method to get access to the underlying data. In the survey, we emphasise obtaining responses to some of our research questions.

- Do organisations have routines for security incident handling and reporting?
- Is there any correlation between handling routines and reporting with respect to the degree and effect between public and private organisations?

The main question is whether security handling and reporting is effectively carried out in the organisations, not just at policy level. In addition, these questions provide answers as to whether there is a difference between security incident handling in public organisations and private businesses.

Contrasted to what can be defined as a security incident in NIST800-61 [16], we can pose relevant questions to the organisations about security incidents. Our research questions are:

- How do organisations define a security incident?
- Are the organisations capable of discovering security incidents?

We have decided to approach a small number of public and private organisations: typical private organisations include large companies within banking, transport, telecommunication, chemical and gambling industry. Public organisations include some municipalities, a county municipality, and an inter-municipal IT operating organisation for three municipalities and large health institutions. The survey provides insight into how these organisations handle their security incidents in practice. We have considered qualitative and quantitative methods or a combination of both as potential methods in this master thesis. As we have chosen a rather small number of organisations, our survey is qualitative in nature. The survey is appropriate for finding differences between private and public sector as well as giving us insight into the practical security incidents handling at those participating in our survey. To get as good response as possible, our selection of organisations has been made by using size as one criterion, personal knowledge of individuals in different organisations as another and using information security branch networks as KINS [22] and ISF [23] as the third.

3.3 Preparation of a checklist

The research question that handles the potential for improvement in the private and public organisations is the following:

- Has the extent of introduction of security incident handling routines and training had any effect on the number of reported security incidents?

We prepared a checklist that the different organisations can use to improve and make their security incident handling and reporting more efficient. By introducing such a checklist we want to contribute to the already-mentioned improvement but also to give the organisations the opportunity to communicate their handling program so that more actual security incidents are reported.

3.4 Defining security metrics

To see if it is possible to measure the effect on security incident handling and get answer to the research question:

- Is it possible to measure how effective security incident handling is?

We use an experiment based on data from the survey. We take our metrics tables that we have developed and fill in data to see if the quality of the metrics is good enough in real life.

4 Security metrics for incident handling

4.1 Introduction

Literature indicates that proper security incident handling and reporting is necessary in order to efficiently handle the threats an organisation faces. It is also important to be able to carry out the appropriate initiatives when a security incident occurs - to reduce consequences and to be able to return to normal situation as soon as possible. For this reason, security incident handling and reporting should be a routine, continuous activity in organisations that have sensitive or critical types of information. The results and contributions in this report can be summarised as follows:

- We have collected information from private and public organisations about how they handle security incidents and how these are being reported. To a slight extent, literature indicates how individual organisations do this and this master thesis can help organisations improve their security incident handling and reporting routines. In addition, the master thesis can illuminate an area that has not been openly discussed much. This is due to the sensitive content each organisation has in its incident handling and reporting practice. For this reason, this master thesis can provide a general approach, useful for all organisations.

- We have asked how organisations define a security incident. Literature indicates that security incidents are broadly and well defined. But a security incident does not have the same significance for all organisations. This master thesis can help different organisations define the most important security incidents and give them tips about what consequences such an incident would have for them.

- We discover through the survey how private and public organisations handle their security incidents in practice. The master thesis can provide answers to whether there are considerable differences in how private and public organisations handle security incidents and how these are reported. For this reason, the master thesis can help the sector that has the greatest potential for improvements.

- We propose using security metrics in order to be able to measure the strength in the organisation's way of handling security incidents. This gives the organisations tools for either determining their own security level or determining security levels of outsourcing vendors, suppliers or 3. party connections. These security metrics can also be used to give management a statistic and a correct picture of how well security incidents are handled.

The master thesis also provides an important input in terms of how public organisations handle security incidents. New legislation, increased focus on privacy protection and the establishment of the (Norwegian) National Security Authority indicates more focus on security in the public sector. For this reason, the master thesis provides controlling and advising authorities' insight into security incident handling and reporting in the public sector.

Major security incidents in the past years have given an increased focus on security work and security investments. However, it is also very important that security investments have a ”Return on investment” (ROI). We need to justify all security investments. Some still claim that we protect us against non-happening threats. To justify these investments, it is important to find a method to measure the effect of the security mechanisms. A well-known management principle [25] is also that “an activity cannot be managed if it cannot be measured”. Research has focused on measuring security and security metrics during recent years. The term ‘security metrics' is, however, a term, which is not mentioned very much in business security. Measurement, follow-up, evaluation, checks, approval and certification are, however, well-known concepts in security standards and statutory regulations [26].

To get overcome today's problems regarding how to give correct answers on the effects on security investments, which effects the security measures have and so on, it is important to find measuring points that also cover how effective the security incident handling is in an organisation. We have in this master thesis also focused on how this can be done. Security metrics are one approach we have found interesting and we therefore define security metrics for that purpose. Our work in this Master thesis is based on a recognised definition of information security, which serves to prevent breaches of confidentiality, integrity and availability [27].

Availability can be defined in the following way [27]:

Availability is ensuring that information or data resources are present and applicable as necessary in accordance with agreed criteria.

Availability can be measured in several places; for example, it must be evaluated if lines of communication are to be included, and if both operative time and response time are to be measured. A metric for accessibility to machines can be measured by “pinging” the machines, whilst a reference measurement may be necessary for a metric for optimal response time, and repeated measurements are carried out in the system under evaluation. In the context of reporting security incidents it can be measured if communication lines are available and if black nodes[1] have the right/enough capacity.

In this thesis, we use the following definition of confidentiality [27]:

Confidentiality is ensuring that information will not be available for unauthorised people or unapproved systems.

Metrics for measuring confidentiality are not easy to find, but access control and access restriction systems can assist in finding cross measurements, which will indirectly be able to provide a good security metric. As an example, one can check if a cryptosystem is in place and if the employees use this system or not.

The following definition of information integrity can be found in [27]:

Integrity is ensuring that information is not changed or destroyed in an unauthorised manner, that information is in agreement with reality and is consistent.

Metrics to ensure integrity, for example in physical and logical data structures can be measured by running consistency checks at given points in time or check figures (hash values) when transferring transaction files.

Good metrics [28] should be easy to understand, simple, and they are not supposed to measure people but processes. Furthermore, they should be result-oriented. According to [29] good metrics must be:

- Specific
- Measurable
- Attainable (Realistic)
- Repeatable
- Independent of time

Metrics can be used to indicate to what extent security targets and requirements are attained [25] and to improve the organisation's security programme and plans. Furthermore, metrics can contribute towards evaluating which security measures are the most effective and assess the security of a specific system, product or process. The metrics can also be an efficient tool for deciding if security measures are to be increased or reduced or whether the security requirements are to be changed.

[1] Black node is here defined as the capacity that solves problems caused by security incidents.

Requirements are made with regard to information security in many contexts, but the tools available for these types of measurement are often inadequate or absent.

4.2 Metrics and Security Incidents

The focus on preventing breaches of security implies that a natural and obvious metric would be to establish requirements for an acceptable maximum number of security incidents within a given period for the individual system. Systems must be classified in accordance with how critical they are for the organisation. Incidents must be classified according to how serious the damage they would cause might be if they occurred.

4.3 Definitions of the Security Metrics

There are several theories regarding how to define and set up metrics. In this thesis, we have chosen to use a template for describing the metrics. We have based our template on NIST terminology [30] and a report written by Orderløkken, Bakås, Hagen at Gjøvik University College [26]. The metrics are described in the form of a table (Table 3).

Table 3 Description of the content of the metric

Attribute	Description
Critical element	Description of what is to be measured, in written form.
Textual explanation	Detailed description of the critical element.
Metric	Definition of the requirement made to achieve the quantitative target the metric is to attain.
The purpose of the metric	A textual description of why this metric is to be used in an SLA[2], i.e. the purpose of the metric.
Requirements	Description of the specific conditions focused on to ensure that the metric is met. This will often be related to which security measures have to be implemented.
Frequency	How often the measurements take place.
Scale	Measurement scales say something about how we measure things and how we interpret the measured values [14]. In practice, this means which tool is used for the actual measurements. Metrics must be quantifiable, as the qualitative concepts are more difficult to measure. Metrics can be quantified by a number, a percentage or an average value.
Formula	Calculations (average value, countings, proportions) which form the basis for calculating the metric.
Data source	Reference to where the data basis from the measurement is taken from. Data can be taken or collected in different ways, for example, automatic methods, by going through documents, mapping, interviews, questionnaires, going through the system configuration or observation.
Indicators	Description of what it means when the metric is attained or not and trends for the measurements.
Qualities of metrics	
Reliability	Description of the method of measurement's precision, i.e. acceptable margin of error, and how reproducible the measurements are. Reliability depends on the operational definition of the metric, for example, degree of detail and completeness. Occasional errors, which are introduced may weaken the level of reliability [9].
Validity	Description of whether what is being measured is the same as what we think we are measuring, and what we are really interested in measuring. Systematic errors in the measurement may weaken the validity of the metric. Errors of validity can be reduced through better metric definition concerning operation and choice of attributes that can be measured. If it is difficult to find direct measurements, which measure what is desired, then cross measurements can be employed. Cross measurements can provide indirect answers to the metric.
Feasibility	Description of how easy/difficult it is to carry out the measurements. There may be technical, administrative or personnel problems, which means that it is not so easy to carry out the measurements.
Areas of conflict	Description of conflicts between, in this case, customer and supplier.

[2] Service Level Agreement.

Customer satisfaction	Description of what the customer achieves by measuring the results via the metric.
Costs and applications	
Costs	Which extra costs are connected with carrying out the measurements and metric. Costs, which will always come in connection with the requirements set up by the metric are not included here.
Specific applications	Description of which areas of application the metric has. In which contexts the metric can be used.

4.4 Different types of security metrics for security incidents handling

In this section we describe how it is possible to build up metrics to measure different aspects of security incident handling and reporting.

4.4.1 Metric for existence and quality of a security incident handling policy

The metric in Table 4 can be used to measure existence and quality of a security incident handling policy.

Table 4 Example of security metric – existence and quality

Critical element	Existence and quality of security incident handling policy,		
Textual explanation	The purpose of a security incident handling policy is to document direction and obligations with regard to implementing security incident handling and reporting, and to communicate it to everyone who has access to the organisation's information and systems.		
Metric	All five questions under Requirements are to be answered YES.		
Aim of the metric	To ensure that the organisation has a security incident handling policy, and that this is in accordance with international standards, for instance, COBIT, ISO 17799, ISF's Standard of Good Practice. [23]		
Requirements		Yes	No
	Is the security incident handling policy documented?		
	Is the security incident handling policy approved by the senior management or head of security?		
	Does your organisation make statistics over number of security incidents?		
	Is the security incident handling policy communicated to all users of information and systems?		
	Is it possible for an independent party to confirm that the security incident handling policy contains the most important elements from a recognised international standard?		
Frequency	Every 2 years or as necessary (e.g. when updating the security incident handling policy)		
Scale	0 to 5 (YES answers)		
Formula	(Number of YES answers / 5) *100		
Data source	Report from independent auditor or another independent party. Head of security.		
Indicators	The target for this metric is 100 %. A lower percentage will imply more security incidents.		
QUALITIES OF THE METRIC			
Reliability	The metric is repeatable and can be measured by independent inspections.		

Validity	The metric will give good answers on the existence of the security incident handling policy. The metric's validity on the quality side is not always easy to measure. Therefore it is not adequate to say that the security regarding the content of the policy is "good enough".
Feasibility	The first four points can be measured easily through checks. The head of security must document for the auditor that an external party has gone through the policy to consider if this satisfies approved international practice.
Area of conflict	Agreement on the selected external party to carry out the audit. If the policy has been communicated adequately to the employees, this may also form grounds for disagreement.
Customer satisfaction	The metric will contribute towards greater customer satisfaction. It is easier for the customer to relate to measurable factors to be able to assess if the supplier has a security incident handling policy and if the quality of that policy is good enough.
Costs and applications	
Costs	The approximate cost is 5 – 10 working days every 2 years: i.e. 3 working days per year.
Specific applications	

4.4.2 Metric for training and attitudes towards security incident handling

The metric in Table 5 can be used to measure how the different organisations train their employees, how they plan attitude campaigns and how many employees have got training.

Table 5 Example of security metric - Training and attitudes

Critical element	Training and attitudes to security incident handling		
Textual explanation	The purpose of training and work on attitudes is to ensure that management, IT managers, users and others with access to systems know the systems and what a security incident is. Additionally, staff must understand what security incident handling is, why it is necessary, and their own responsibilities regarding security incident handling.		
Metric	100 % of the employees who have access to the systems go through security incident handling training on an annual basis, in accordance with an established plan.		
Aim of the metric	To ensure that those with access to our systems know what security incidents are and why it is important to report them. This is in addition to ensuring that employees' attitudes to security are kept at a good level. The employees who contribute towards operating our systems must know the content of the security incident handling policy and obey it.		
Requirements		Yes	No
	1.Are measures dealing with attitudes planned on an annual basis?		
	2. Will the employees be given training concerning security incident handling so that they can handle and report security incidents?		
	3. Number of employees with access to our systems?		
	4. Number of employees who have participated in this year's security incident handling training		
Frequency	Annually		
Scale	0 – 100 %		
Formula	(Number of employees with access / Number of employees who have received training) * 100 and yes on question 2.		
Data source	Report from head of security		
Indicators	The target for this metric is 100 %. It is accepted that it cannot be documented that all employees have received training. However, what can be documented is which measures are to be taken and that employees who are involved in working with our systems have had the opportunity to receive training, that time has been set aside for this and that the training is targeted at the employees.		
QUALITIES OF THE METRIC			
Reliability	The metric is repeatable to a certain extent. There are probably different		

	measures from year to year, and these have different levels of measurability. The level of reliability of the measurements will vary from year to year.
Validity	The metric will give good answers as to whether there are plans for training and work on security incidents. The level of quality will be difficult to measure. For security to give information about this, it will be necessary to measure the expertise of the employees concerned before and after training is carried out each year. This will be demanding on resources.
Feasibility	Certain training incentives are difficult to measure, so, for example, some “drips” on the intranet can be good reminders about security incident handling, but if this is only on the front page it will not be possible to measure how many people actually read it.
Area of conflict	The quality of training is a possible area of conflict. This can be measured, but is very demanding on resources.
Customer satisfaction	The metric will be able to contribute to feeling more secure, and that the organisation focuses on security.
Costs and applications	
Costs	Any extra costs when developing attitude-related measures to count the employees who participate in or carry out training. This will vary with the kind of measure carried out.
Specific applications	At annual status meetings with the head of security.

4.4.3 Metric for effectively handling of security incidents

The metric in Table 6 can be used to measure how effectively security incidents are dealt with.

Table 6 Example of security metric – Effectively handling of security incidents

Critical element	Effectively handling of security incidents		
Textual explanation	To ensure that security incidents, i.e. breaches of confidentiality, integrity and interruptions in availability are dealt with in the most efficient way possible to minimise the consequences for the organisation, and reduce the probability of something similar happening again.		
Metric	No interruption in availability lasts longer than the defined critical time for the system. No information defined as confidential or company internal gets into the hands of unauthorised people. No data or information is manipulated or outdated, as defined in the systems' classification. All incidents are reported to the organisation's reporting system.		
Aim of the metric	The purpose of the metric is to follow up security incidents in connection with interruptions in availability, confidentiality and integrity, in addition to ensuring that the customer gets information about all incidents.		
Requirements		Yes	No
	Is there a process for dealing with security incidents?		
	Are all known security incidents registered and reported?		
	Are security incidents documented immediately?		
	Is the pattern of incidents assessed so that any common problems can be revealed?		
Frequency	Monthly		
Scale	0-4 yes answers.		
Formula	(Yes on all 4 questions/4)*100		
Data source	Incident report from the employees and sensors. Own documentation of incidents.		
Indicators	The target for this metric is 100%. A lower percentage will imply that routines for security incident handling have to be improved.		
QUALITIES OF THE METRIC			
Reliability	The metric is repeatable. The management and employees agree beforehand on criteria for reporting, as well as on the form for reporting incidents. The same form is sent to the management each month.		
Validity	The metric, as well as one's own experiences in error situations will provide clear indications as to whether the supplier deals with security incidents in accordance with good practice.		
Feasibility	The weakness of the metric is if the supplier, vendors or others really wants to document all incidents. Some incidents are difficult to intercept, such as breaches of confidentiality. Operational personnel are not normally		

	enthusiastic about documentation.
Area of conflict	The definition of security incidents can be a subject for discussion. Other incidents can be forgotten with regard to documentation.
Customer satisfaction	The metric contributes towards giving the head of security a total overview of which security incidents have occurred. All security measures are carried out. Over time, the head of security thereby will get an indirectly measured report of whether his organisation has a good level of security.
Costs and applications	
Costs	No information above and beyond what is common practice for information security is necessary for the metric. There are no extra costs related with this metric.
Specific applications	Monthly internal meetings at the customers' premises. At monthly status meetings with the supplier. When renegotiating contracts.

4.5 Implementation of security metrics

To give security managers or others responsible for security, a possibility to report to management, board or into own reporting chain on the security status, it is very important to have statistics, documented effects, cost savings or other measurable elements to report on. By making use of these examples of security metrics, the reporting officer in an understandable way, can give management a good statistics. This can again lead to better understanding of security work and easier approval of security investments. It is also a tool for measuring outsourcing vendors, or measuring the security status in own organisation.

5 Experimental work

5.1 Survey

In this master thesis we aim to find out if we can get answers to the research questions. The research questions are related to handling and reporting security incidents. To find answers to these questions, we have made a survey. The survey has been sent out to 35 different organisations both public and private. The organisations were selected with an aim to get the best mix between different branches, different sizes and also different public organisations. We have received 22 answers, 2 did not want to participate due to workload, 20 answers were positive with filled in answers. Of these 11 were from public organisations and 9 from private organisations. This gives a response rate of 62,9%.

5.2 Survey answers

In this chapter we outline the answers given from the participants in the survey with short statistics and comments. The more detailed results are described in Appendix D.

5.2.1 Part 1: Policy and routines

The questions in the first part deal with policy and routines. This part consists of 11 questions. The questions also include if the organisations have any form of Computer Security Incident Response Team (CSIRT) (see Appendix D). It is important to understand if the organisations have policy and routines in place when we later on start to analyse the results from the survey. The detailed data from the answers can be found in Appendix D.

95% of the organisations have a security policy. 100% of the organisations that have a security policy also include information security in the policy.

94,7% of the organisations that have a policy answer that the policy has been approved by the top management. 5,3% of the organisations answer that their policy has not been approved at all.

All the private organisations have a policy, their policy also include information security and are all approved by the top management. 90.9% of the public organisations have a security policy.

International standards

We asked if the organisations follow an international standard for information security. The results from all the responders showed that 50% of the organisations follow an international standard (i.e. BS7799, ISO17799, ISF standard of good practice etc). If we divide these results between private and public sector, we find a significant difference.

Figure 3 shows the difference in how private and public organisations follow or do not follow an international standard for information security.

As Figure 3 shows, only 18,2% of the public organisations follow an international standard. 88,9% of the private organisations follow an international standard.

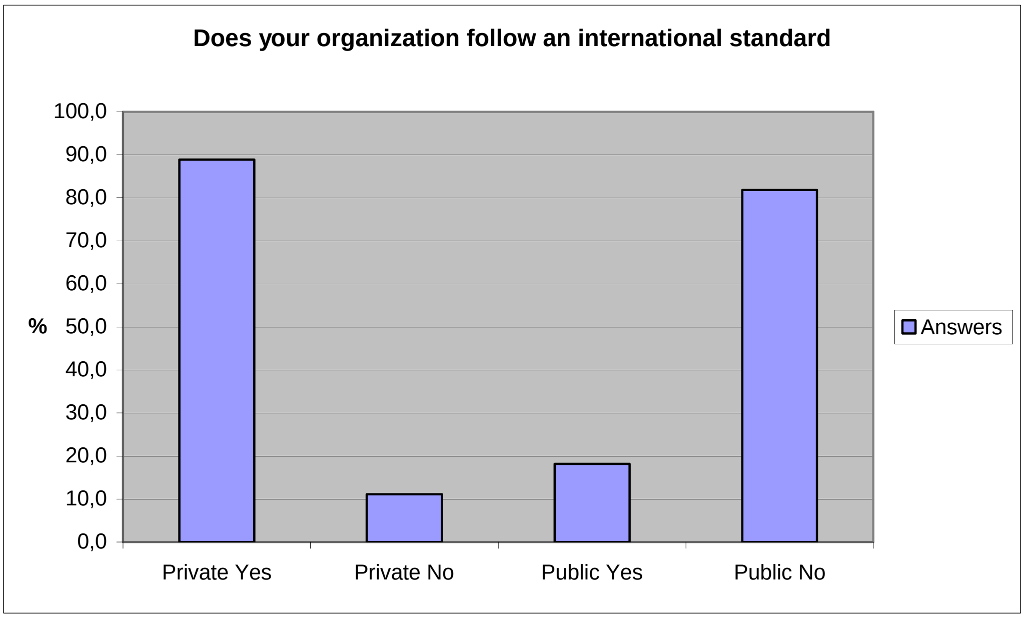


Figure 3 Use of international standards.

Incident handling policy.

We have also asked if the organisations have policy/routines for security incident handling. 80% of the responders answer that they have an approved policy/ routine. We can also see here a difference between private and public organisations.

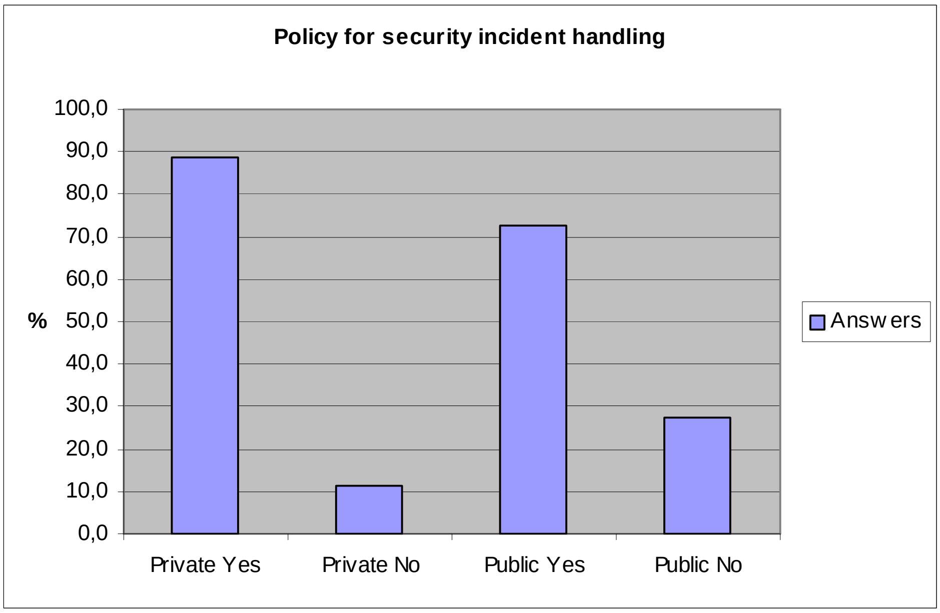


Figure 4 Policy for security incident handling.

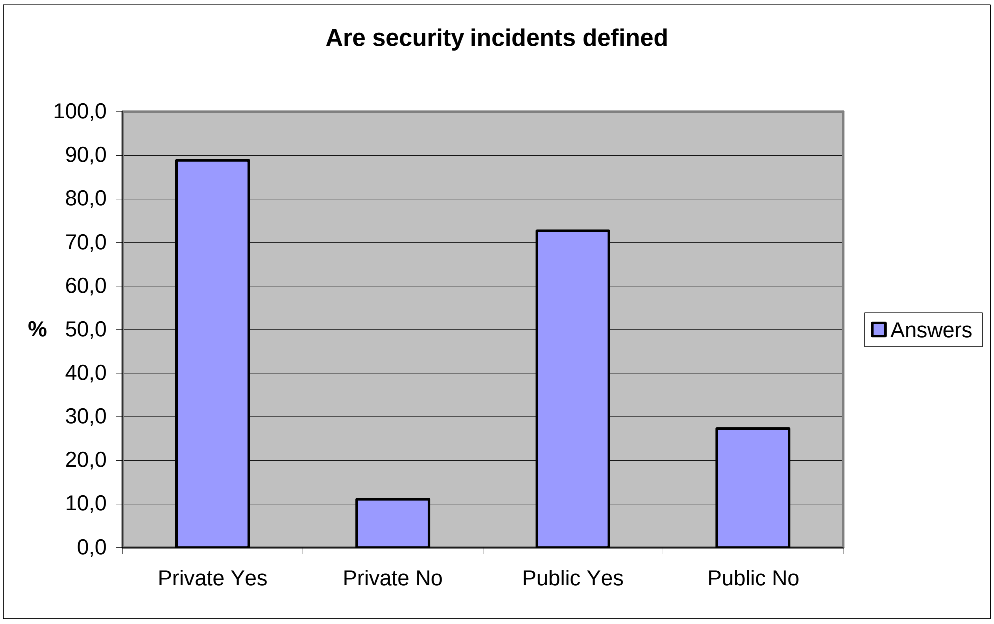
The difference as seen in Figure 4 indicates that public organisations are less provided with policies regarding security incident handling than private organisations. The difference is however not significant.

Definitions

80% of the organisations answer that they have defined what a security incident is. The difference between private and public organisations is as shown in Figure 5.

There is also a difference here between private and public organisations. Private organisations have more responders saying that they have defined security incidents than public organisations.

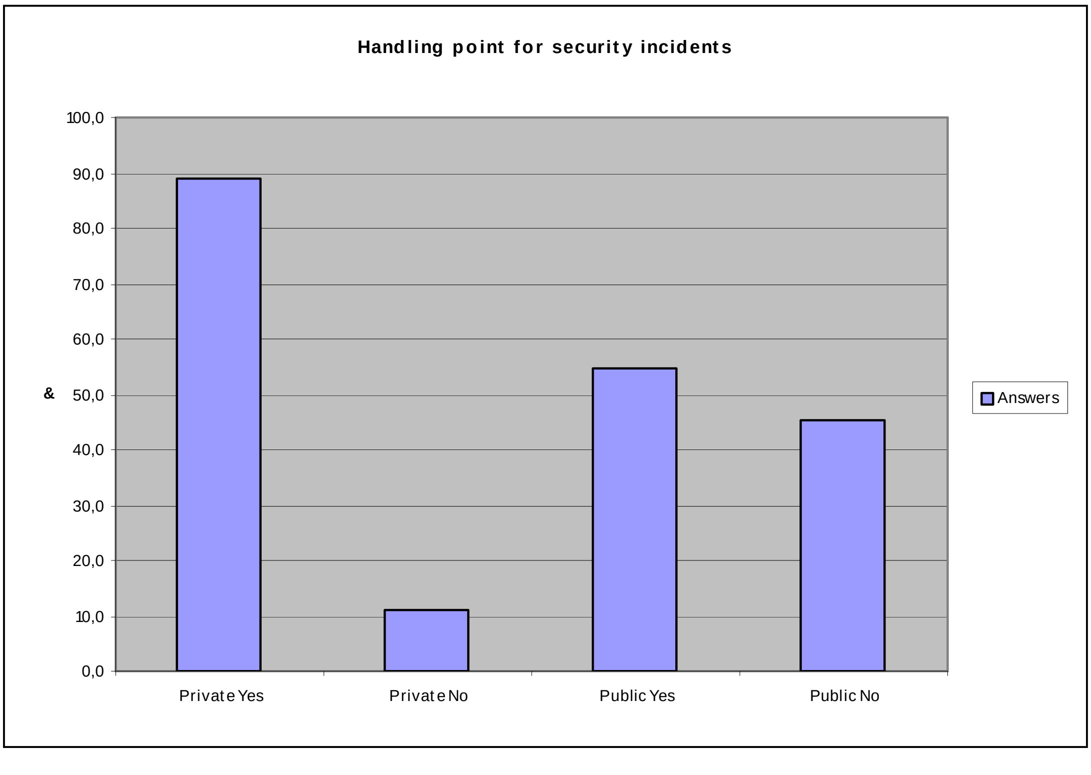
Figure 5 Are security incident defined.



Handling point.

We asked if the organisations have a handling point for security incidents (i.e. (Tiger Team, Computer Incident Response Team (CIRT), IT-Department, security manager etc.) 70% of the organisations answer that they have a handling point.

Figure 6 Handling point for incidents



The difference between private and public organisations is in this case big. 8 out of 9 private and only 6 out of 11 public organisations have a handling point for security incidents see Figure 6.

Whistle blowing[3] and statistics.

The last questions in the first section handled about whistle blowing and statistics. - Do the organisation have a whistle blowing system and do they make statistics over security incidents. Both private and public organisations scored low on the whistle-blowing question. Only 25% of the organisations have a whistle blowing system as shown in Figure 7.

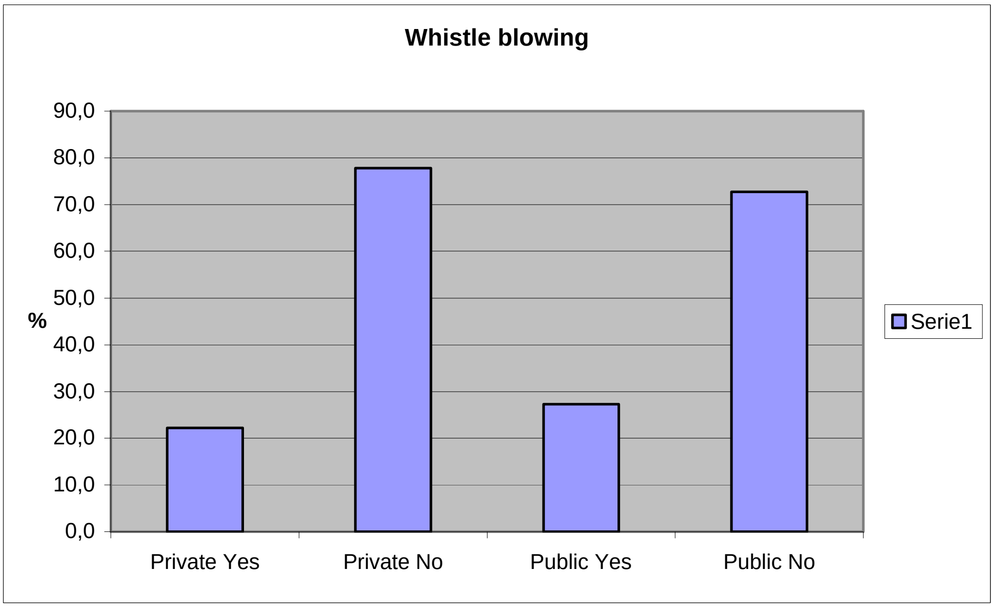


Figure 7 Whistle blowing.

60% of the organisations make statistics over security incidents. There is also a difference here between private and public organisations.

Of the private organisations, 77,8% answer that they make statistics, 45,5% of the public organisations make statistics, see Figure 8.

[3] Whistle blowing is defined as an anonymously reporting system in an organisation.

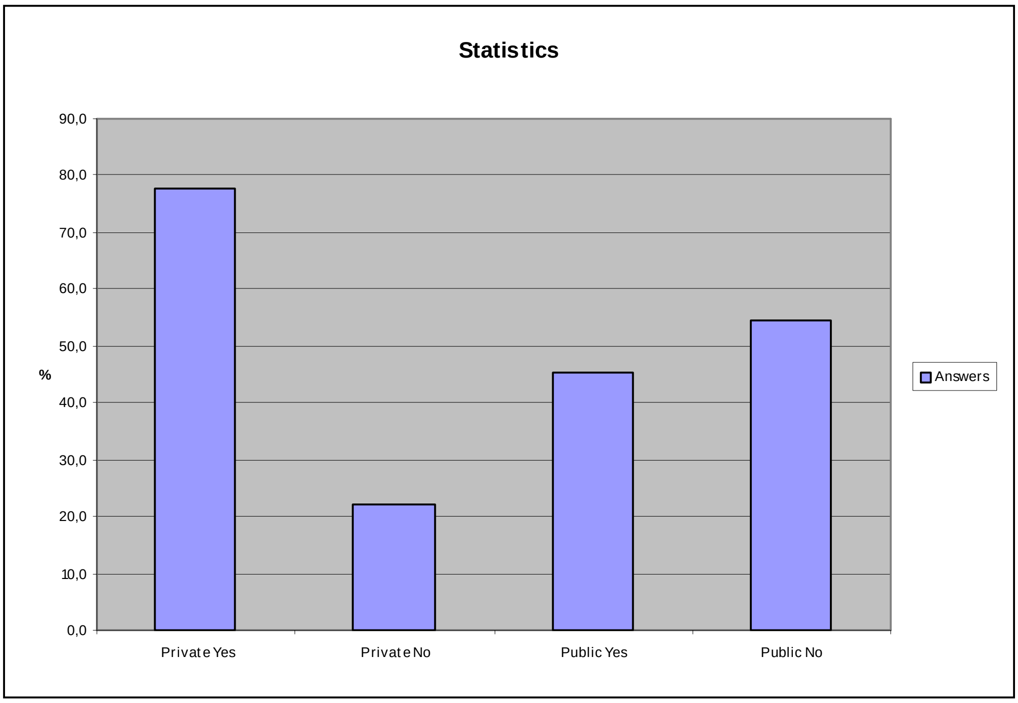


Figure 8 Statistics

5.2.2 Part 2: Handling of security incidents in practice

In this section of the questionnaire, we asked different questions regarding how the organisations handle security incidents in practice. The responders were asked to grade their answers from 1-5, where 1 corresponds to “to a little extent” and 5 corresponds to “to a large extent”. There was also one mark for answering that they do not know the answer.

To get the data from these questions, we have classified the data into three categories. The answers in the scale 1-2, scale 3 and scale 4-5 have been calculated.

We asked the responders to see the questions from their point of view and from their knowledge of their own organisation describe in what extent the following statements were true. Table 7 shows the average grading from all the organisations, private and public. As the figures show, there is a difference between private and public organisations especially when it comes to the question if the organisations are capable of reporting security incidents.

From your knowledge in own organisation, to what extent:

Nr.	Question	All	Private	Public
Q12	Is your organisation capable of discovering security incidents?	3,20	3,89	2,64
Q13	Is your organisation capable of reporting security incidents?	3,35	4,22	2,64
Q14	Is your organisation capable of reacting on security incidents?	4,05	4,67	3,55
Q15	Does your organisation realize the threats you are facing within the information security area?	4,00	4,44	3,64
Q16	Is Your organisation risk managed (i.e decisions that are taken are based on risk assessments).	3,50	4,11	3,00

Table 7 Handling security incident in practice.

1 corresponds to “to a little extent” and 5 corresponds to “to a large extent”.

Figure 9 shows that in all cases the public organisations score lower than the private organisations.

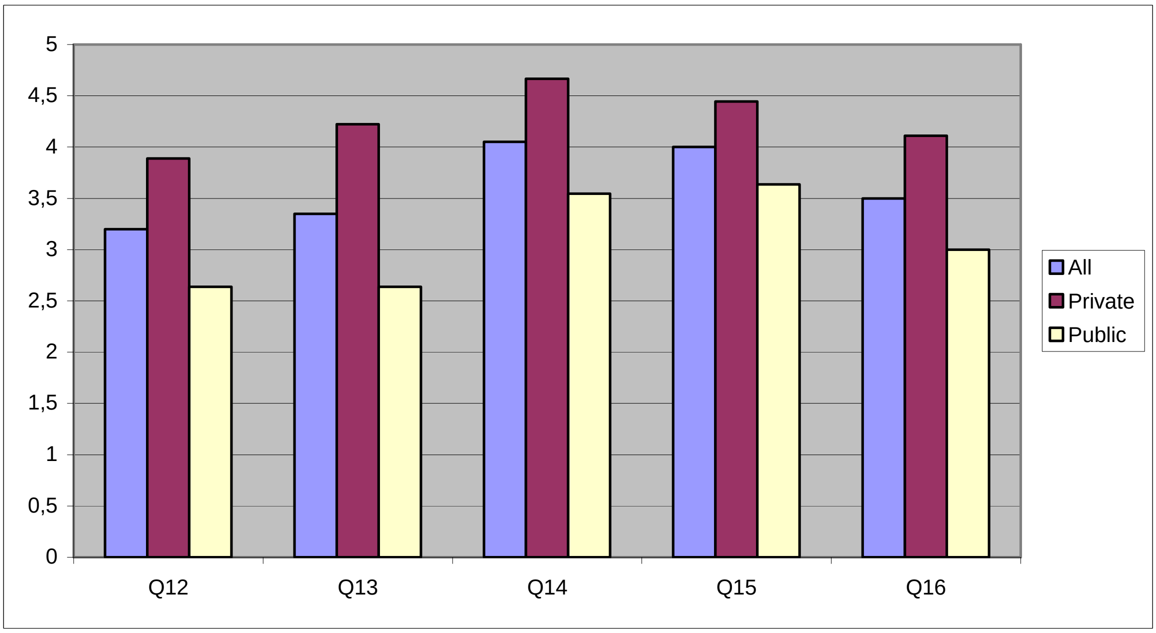


Figure 9 Handling incidents in practice.

If we take the answer and find out how the organisations responded to question 13, which had the biggest difference between private and public, we found that 88,9% of the private companies answered that their organisation in large extent were capable of reporting security incidents. Only 9,1% of the public organisations answered that their organisations were capable to report security incidents to a large extent (Figure 10).

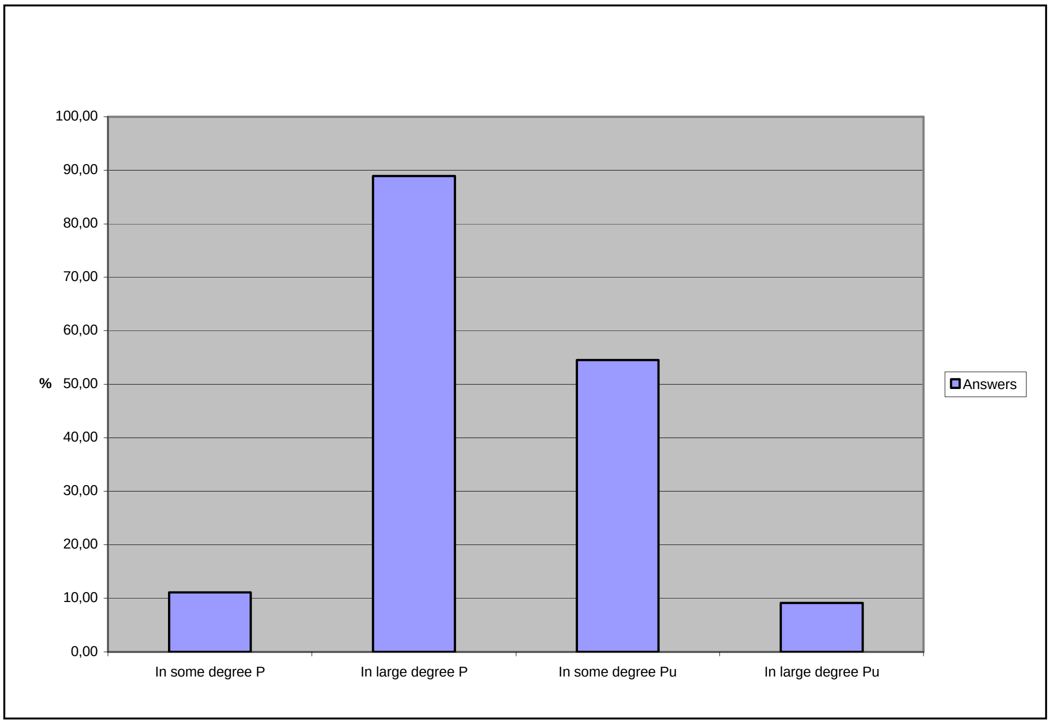


Figure 10 Reporting capability

5.2.3 Part 3: Definitions of security incidents

We asked in this section if the organisations from their own definitions, or based on their own experience, could point out 10 examples of security incidents. 15 organisations answered this question. Many gave almost the same definitions. In Table 8 we have listed some of the most used definitions.

Table 8 Security Incidents definitions

Security Incidents defined by the organisations:
Virus attacks
Hacking
Breach of policy, regulations and laws
Loss of sensitive or classified information
Illegal downloading
DoS/DDOS attacks
Misuse of IT equipment
Deactivated security mechanisms
Fire

Theft
Lending out username and password
Sending sensitive/classified email to unauthorised recipients
Unauthorised security scanning
Phishing
Threats against organisation or staff
Human errors
Fraud
Unauthorised use
Power failure
Unauthorised tunnelling through firewall
Breach of professional secrecy

There were no big differences between public and private organisations regarding this matter. The same definitions are used in both organisations. Two common incidents from the public domain were breach of professional secrecy and loss of sensitive or classified information.

5.2.4 Part 4: Follow-up of security incidents

In this section we asked the organisations how they follow up their security incidents. We also included questions regarding statistical data to find out if they where capable of detecting security incidents.

Tools

55% of the organisations have tools for handling and reporting security incidents. 45% have no tools for handling and reporting security incidents.

45,5% of the public and 66,7% of the private organisations have tools for handling and reporting security incidents.

There are different vendors and different systems in place in the organisations that answer that they have tools. Remedy, Action request, Service desk, TQM[4] Partner and some self-made systems are in use.

Reporting point

On this question, 40% of the organisations answered that they report to one role in the organisation. The role they report to differs between management, security manager and the closest superior.

[4] Total Quality Management

55% of the organisations report security incidents to different roles in their organisation. They report to between 2-4 different reporting points in each organisation. 5% of the organisations do not report to any role in the organisation.

Reporting structure

60% of the organisations report into a tree structure, meaning that the person reporting the incident reports to a person in a defined chain.

55% of the organisations report into a matrix structure meaning that they report to different roles or persons in their organisation. If we take the difference between private and public as shown in Figure 11, we get the following result:

55,6% of the private and 63,6% of the public organisations report in a tree structure.

77,8% of the private and 36,4% of the public organisations report into a matrix structure.

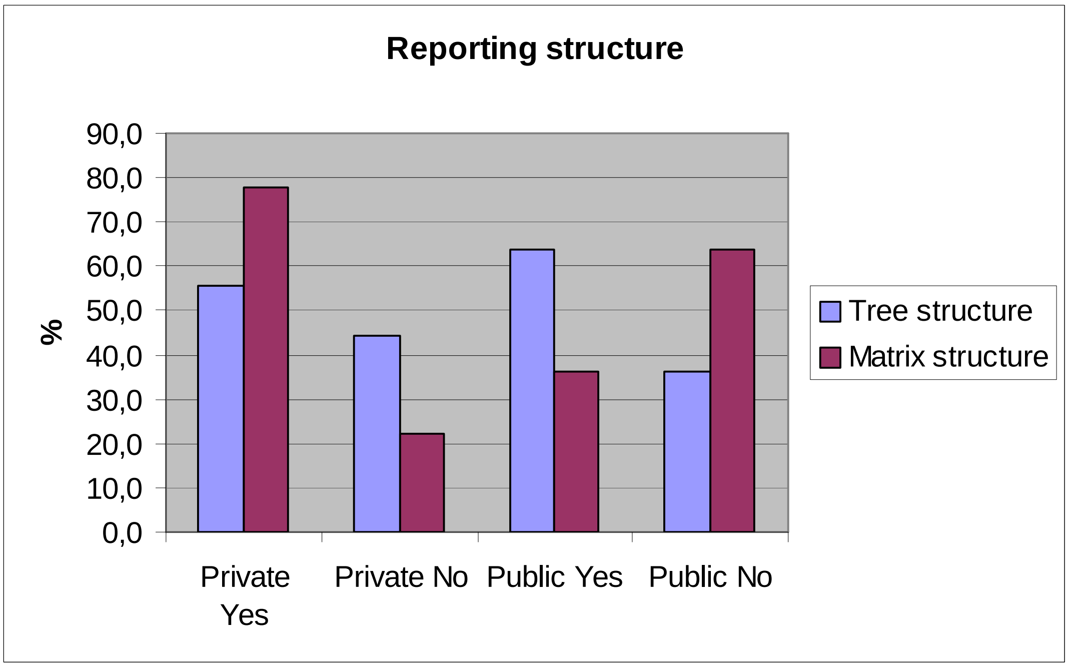


Figure 11 Reporting structure.

From the answers to the questions 20 and 21 we can find that 27,3% of the public and 11,1% of the private organisations do not report either into a tree structure or a matrix structure. We can also find that 35% of the organisations answer that they report into both a tree structure and a matrix structure.

Capacity

40% of the organisations answer that capacity is a topic in their organisation.

55,6% of the private and 27,3% of the public organisations think that capacity is a topic.

Number of security incidents reported.

We asked the organisations how many incidents were reported, into reporting chain and to the police. For the reporting chain, our scale was:

- 0-24 incidents
- 25-49 incidents
- 50-99 incidents
- Over 100 incidents.

35% of the organisations had 0-24 incidents reported.

No organisations reported between 25 and 49 incidents.

15 % of the organisations had 50-99 incidents reported.

10% of the organisations had over 100 reported security incidents.

40% of the organisations did not know how many incidents were reported.

26,3% of the organisations did not know how many security incidents were notified to the police.

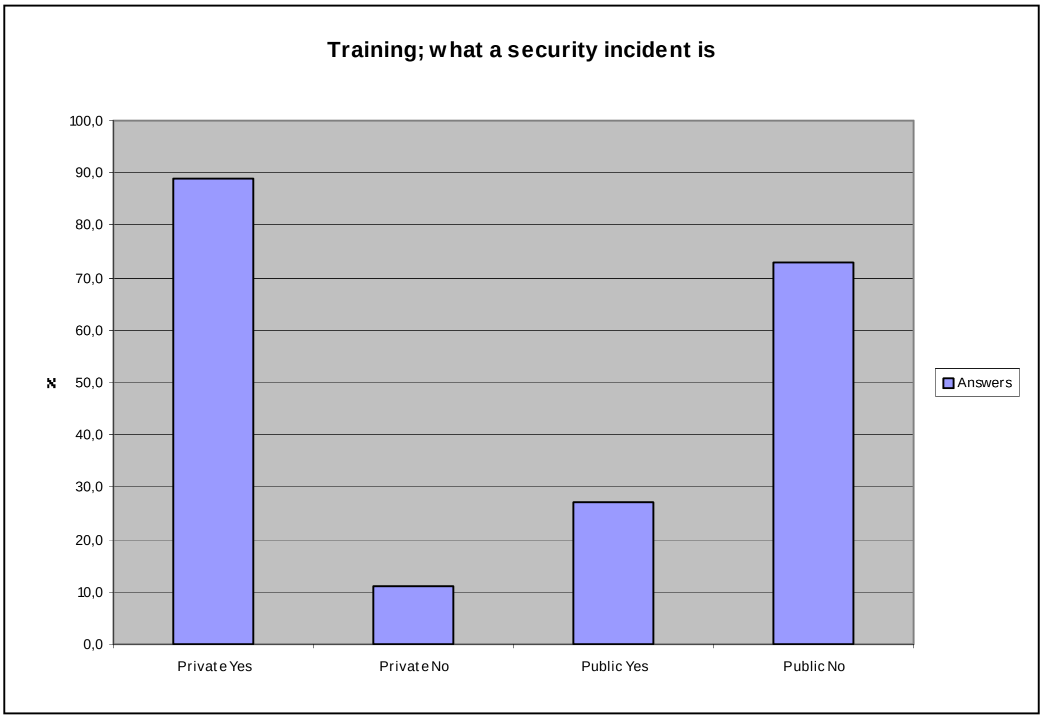
73,7% of the organisations answering the question regarding police notification had numbers of notifications between 0-5.

5.2.5 Part 5: Training

In this section, we have asked the organisations abut training within the security incident area. First, we asked questions about what the employees had got training in.

55% of the organisations have training in what a security incident is. If we look into the difference between private and public organisations we find again a difference as shown in Figure 12. Here we find that 88,9% of the private organisations have training in what a security incident is. Only 27,3% of the public organisations have such training.

Figure 12 Training: What a security incident is.



We also wanted to find out if the employees in the organisations had training in what to do if they discover a security incident.

75% of the organisations say that the employees have training in what to do if they discover a security incident.

54,5% of the public and 100% of the private organisations say that their employees have training in what to do if they discover a security incident.

When it comes to training in where to report security incidents we find the same result. All the private organisations have training but only 54,5% of the public organisations have this type of employee training.

Effects - with or without training

The responders were asked to grade their answers in questions 29 – 34, regarding how the responders mean that their employees handle security incidents. The scale was from 1-5 where 1 corresponds to “to a little extent” and 5 corresponds to “to a large extent”. There was also one mark for answering that they do not know the answer. To get the data from these questions we have put the data into three categories. The answers are put in different scales; scale 1-2, scale 3 and scale 4-5 have been calculated. Table 9 shows the average grading from all the organisations, private and public. Questions 32 - 34 were answered by 65% of the organisations. 54,6% of the public and 77,8% of the private organisations answered these questions referring to if education has been given or not.

Nr.	Regardless of training has been given or not, in what extent:	All	Private	Public
Q29	Is your employee aware of how to handle security incidents?	2,95	3,44	2,55
Q30	Do they know where they can find information about handling of security incidents?	2,80	3,33	2,36
Q31	Do they know where to report security incidents?	3,15	3,56	2,82
	If training has been given, to what extent gives that:			
Q32	A significant effect on the number of reported security incidents.	3,30	3,00	3,50
Q33	Increased focus on security incidents.	3,45	3,40	3,50
Q34	Better management support/anchoring for security work.	3,64	3,60	3,67

Table 9 Training and effects.

Table 9 shows that there is a big difference between how private and public organisations think that the employees deal with security incidents. Based on the independence on the answer to the question if education has been given or not, the public average score is much lower than what we find in the private domain. If education is given, we find that there is no big difference between private and public organisations on how they think this will affect the security incident focus and handling.

5.2.6 Part 6: Handling of security incidents and its effect.

In this section, we have asked the organisations about how their handling of security incidents affects their security work. There are several different questions and we asked how they weighted the following statements: The scale uses 1 for “does not agree” and grades the answers up to 6 that means “totally agree”.

Question 35: - All the employees in my organisation knows what a security incident is.

42,1% of the organisations answer that they do not agree with this statement (answers 1-2 in the tickboxes). 52,6% answer that they to some extent agree (3-4 in the tickbox). 5,3% of the organisations totally agree (5-6 in the tickbox).

22,2% of the private and 60% of the public organisations say that their employees know to a little extent what a security incident is. 66,7% of the private and 40% of the public organisations say that they to some extent know that. 0% of the public and 11,1% of the private organisations say that all their employees know what a security incident is. Table 10 shows the average score. 1 corresponds to "does not agree" and 6 corresponds to "totally agree"

Nr.	Question (Grading 1-6)	All	Private	Public
Q35	- All the employees in my organisation know what a security incident is.	2,75	3,33	2,27
Q36	- All the employees in my organisation know where to report security incidents.	3,25	4,00	2,64
Q37	- We are capable of detecting security incidents	3,6	4,33	3,00
Q38	- It is easier to get acceptance for security investments if we have an overview of security incidents.	4,68	4,89	4,50
Q39	- A good handling of security incidents will increase the security level in our organisation.	5,15	4,89	5,36
Q40	- If we have an overview of security incidents we could enforce security measures more effectively.	5,05	5,00	5,09
Q41	- You will never get a total overview over security incidents and security violations.	4,7	4,56	4,82
Q42	- It is not a custom in my organisation to report security incidents.	2,8	2,67	2,91
Q43	- You can throw suspicion on yourself when reporting security incidents.	2,1	2,11	2,09
Q44	- I shall never report a security violation committed by a colleague.	1,6	1,78	1,45

Table 10 Handling security incidents in practice

Figure 13 shows a graphical display of the answers to questions 35 to 44.

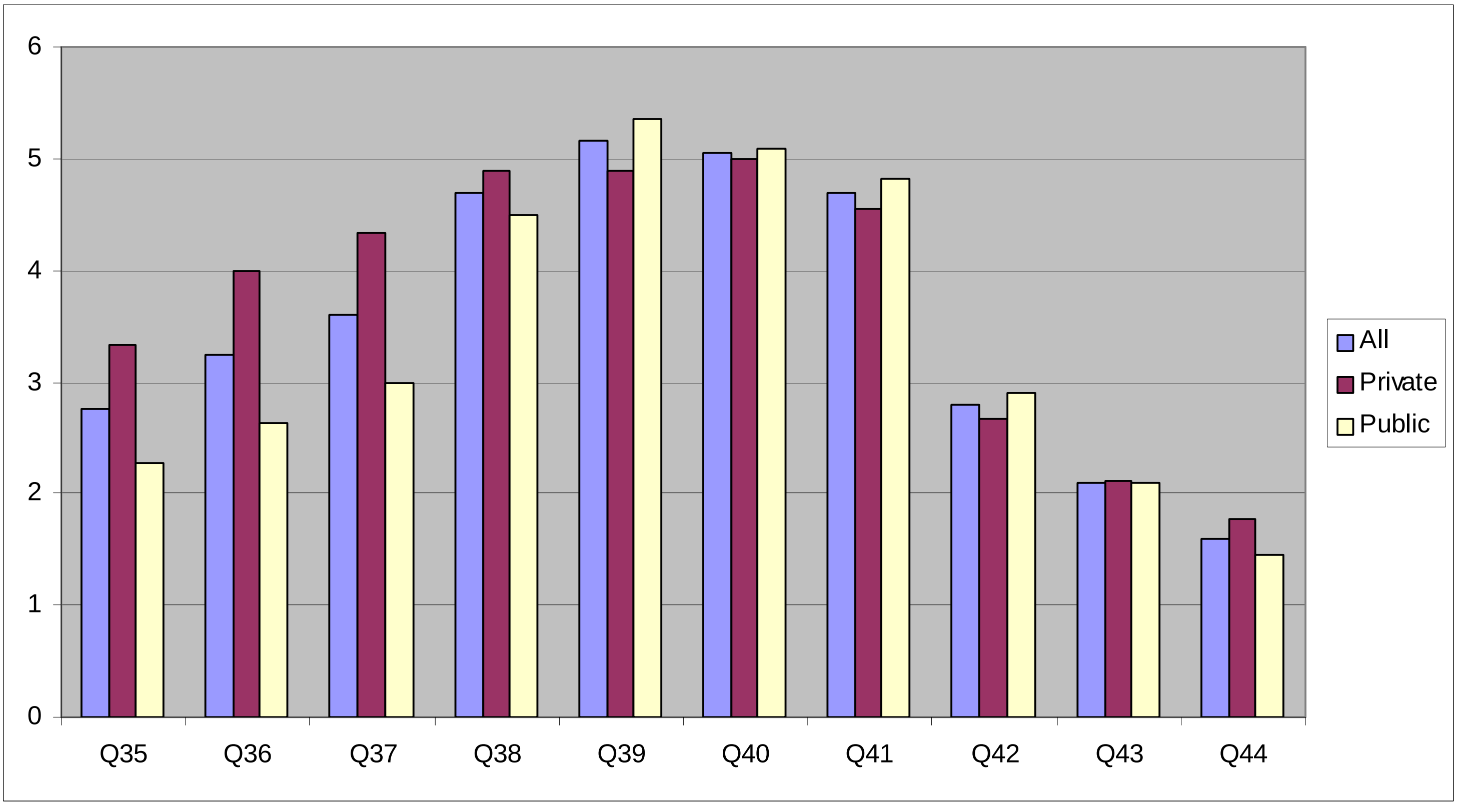


Figure 13 Handling security incidents in practice - chart

5.2.7 Part 7: About the organisation

In this section, we asked the responders about their role, who they were reporting to, the size of the organisation and in what branch they were operating.

The majority of the responders are security managers or IT security managers. Some are security advisors or ICT advisors.

The majority of the responders report to management functions such as security director, CEO or IT Director.

Table 11 shows the size of the organisations responding to the questionnaire.

Number of employees	Number of organisations
0 –199	1
200 – 999	4
1000 - 4999	3
Over 5000	12

Table 11 Size of responder organisations

When it comes to different branches the responders belong to, Table 12 shows which branches the different responders belong to.

What branch does your organisation belong to?			
1. Bank, finance, insurance	1	7. Public sector	11
2. Chemicals, health	1	8. Retail trade	
3. Energy, power		9. IT supplier	2
4. Industry/ production		10. Telecommunication	1
5. Media, post	1	11. Transport	1
6. Process industry		12. Other (Please specify):	2

Table 12 Branches

5.3 Reliability and validity

The questionnaire was designed so that it should be possible to reproduce the results and measurements. The validity of the results seems satisfactory. The questions are easily understood and the responders are highly skilled and have positions in their own organisations that give them the possibility to answer this type of questions. In the cover letter it is stated that the survey gives full anonymity and that also gives room for more honest and accurate answers.

If we study literature within the statistics area, our number of responders may seem to be low. 35 organisations were asked, 2 did not want to give answers, 20 answered the survey, and this gives a response rate of 62,9%. With this number of responders it is important to take exceptional care about the procedures involved when going through the data. To present statistics data from this sample, we have to state the numbers of responders [33].

The survey was sent to Norwegian organisations with more than 100 employees. The selection was also done to get almost equal number of private and public organisations to respond.

5.4 Ethical and legal considerations

According to the lecturer in "Vitenskapelige metoder" (Scientific Methods) one must ensure to review the ethical and legal aspects of the project [24]. In this thesis, it is primarily considerations concerning confidentiality that must be reviewed. Security questions, which are posed in this project, are of a sensitive nature and for this reason the results must be made anonymous. The data must be protected so that unauthorised persons do not gain access to the collected data.

There is a requirement to do this voluntarily in this research project, and this requirement also applies in terms of collecting personal information. Pursuant to the (Norwegian) Personal Data Act, consent shall be given to enter personal information into a register. In this thesis names, functions, and employers will be visible in the collected data, so plans to delete the data must be made after the completion of the thesis.

5.5 Security metrics used in security incident handling

As mentioned in Chapter 4, security metrics may give a benefit for organisations dealing with security incidents. Both Management level, IT department and security department can obtain good information and statistics from security metrics that focus on security incident handling. This can be used for justifying security investments. Such metrics may also be useful for all reporting purposes both internally and externally. Obviously the metrics can also be used to establish requirements for an acceptable maximum number of security incidents within a given period for the individual system.

In this master thesis we have developed several security metrics to be used for these purposes. Measuring security is very difficult and all new ways of dealing with this type of measures are of great value. We have defined the following metrics:

- Existence and quality of security incident handling policy
- Training and attitudes to security incident handling
- Effectively handling of security incidents

To see if these metrics can be applied to real life functions we have used real life data to evaluate each metric. We have chosen data from the survey from two organisations, one private and one public. The data have been put into the formulas in the metrics and the results are presented in the next Section.

5.5.1 Existence and quality of security incident handling policy

To see if our security metrics work, we have used data from two organisations answering the survey. The two organisations we have collected data from have over 5000 employees, one from the private sector and one from the public sector.

Table 13 Public organisation

Critical element	Existence and quality of security incident handling policy,
Textual explanation	The purpose of a security incident handling policy is to document direction and obligations with regard to implementing security incident handling and reporting, and to communicate it to everyone who has access to the organisation's information and systems.
Metric	All five questions under Requirements are to be answered YES.
Aim of the metric	To ensure that the organisation has a security incident handling policy, and that this is in accordance with international standards, for instance, COBIT,

	ISO 17799, ISF's Standard of Good Practice.		
Requirements		Yes	No
	Is the security incident handling policy documented?	X	
	Is the security incident handling policy approved by the senior management or head of security?	X	
	Does your organisation make statistics over number of security incidents?	X	
	Is the security incident handling policy communicated to all users of information and systems?		X
	Is it possible for an independent party to confirm that the security incident handling policy contains the most important elements from a recognised international standard?	X	
Frequency	Every 2 years or as necessary (e.g. when updating the security incident handling policy)		
Scale	0 to 5 (YES answers)		
Formula	(Number of YES answers /) 5 *100		
Data source	Report from independent auditor or another independent party. Head of security.		
Indicators	The target for this metric is 100 %. A lower percentage will imply more security incidents . Few specific requirements have been set up.		
QUALITIES OF THE METRIC			
Reliability	The metric is repeatable and can be evluated by independent inspections.		
Validity	The metric will give good answers on the existence of the security incident handling policy. The metric's validity on the quality side is not always easy to measure. Therefore it is not good to say that the security regarding the content of the policy is "good enough".		
Feasibility	The first four points can be measured easily through checks. The head of security must document for the auditor that an external party has gone through the policy to consider if this satisfies approved international practice.		
Area of conflict	Agreement on the selected external party to carry out the audit. If the policy has been communicated adequately to the employees, this may also form grounds for disagreement. It is difficult to document in a way which requires few resources.		
Customer satisfaction	The metric will contribute towards greater customer satisfaction. It is easier for the customer to relate to measurable factors to be able to assess if the supplier has a security policy and if the quality of that policy is good enough.		
Costs and applications			
Costs	The approximate cost is 5 – 10 working days every 2 years: i.e. 3 working days per year.		
Specific applications			

This metric indicates that there is a lack of training in this organisation. From the formula this public organisation get 80% score. The target is 100%.

For the private organisation the result is:

Table 14 Private organisation

Requirements		Yes	No
	Is the security incident handling policy documented?	X	
	Is the security incident handling policy approved by the senior management or head of security?	X	
	Does your organisation make statistics over number of security incidents?	X	
	Is the security incident handling policy communicated to all users of information and systems?	X	
	Is it possible for an independent party to confirm that the security incident handling policy contains the most important elements from a recognised international standard?	X	
	Is the security incident handling policy documented?	X	

The metric in Table 14 shows that this private organisation fulfils all the requirements for this metric. The result is 100% score.

6 Discussion

The main focus of this master thesis is to find if there is a difference between how theory describes security incidents and how organisations carry out security incident handling in practice.

The data from the survey provided a lot of information that can be used in different statistical ways, but as mentioned in section 5.3 the number of responders were to small to give any results without stating the number of responders which is 20. To get into the subject it is also important to find out if the hypothesis mentioned in Section 1.5 is true. We wanted to find out if there is a difference between how private and public organisations deal with security incidents.

The theory concerning handling and reporting of security incidents described in Chapter 2 gives the organisations policies, routines and guidelines how to organise their security incident handling efforts. Our survey shows that the organisations participating, in many areas do not follow all the guidelines for a proper security incident handling. One major finding is, however, that private organisations in most cases have security incident handling policies and routines in place. Public organisations have a security policy in place but in fewer occasions a security incident handling policy is in place. If we take this information into consideration when we analyse how the different organisations answer questions regarding how they think their organisation deals with security incidents in practice, we found several interesting findings that are discussed further on in this Chapter.

Most of the statistic details that came out of the survey conclude with difference between how public and private organisations handle security incidents. In some areas there are no major differences. If we take security policy we found that almost all organisations had a security policy and also included information security in the policy. We found however a major difference when we asked if they followed an international standard for information security. 8 out of 9 (88,9%) private organisations follow an international standard for information security but only 2 out of 11 (18,2%) public organisations follow an international standard. To explain this, we point out that information security has not been a top priority within the public domain in the past years [22]. However, new laws, more focus on sensitive data and the personnel act, integration of IT systems and services have to be met by the public organisations too. This can again give the public domain the attention needed for implementing good routines and practices for handling and reporting of security incidents.

Training is a considerable part of a good security incident handling program. The employees need to know what to do if a security incident occurs. They also need to know what a security incident is and where to find information about the handling policy and the different routines describing security incident handling and reporting. Our survey shows that the private organisations state that they give this type of training. The public organisations, however, are not at the same level. Only 27,3% state that their employees are trained in what a security incident is. A little over 50% of the public organisations are trained in what to do or where to report the incident. When we take these data and measure against what the organisations have answered on what level they think their organisations are at in practice, we find interesting answers. The private organisations who stated that they had training in what to do if they discover a security incident answer here that in their organisation the employees get an average score of 3,44 out of 5 (1 corresponds to "to a little extent" and 5 corresponds to "to a large extent") on this matter. This indicates that either the training has not been effective enough or that the employees do not follow established routines. The trends we have seen in he public domain also continue here. The public domain gets an average of 2,55. The same results also apply to all questions related to where the organisations stand in practical handling of security incidents. This indicates that in most public organisations they need to improve both documentation and training.

Besides giving answer to the hypothesis, our master thesis survey also gave good answers to our research questions. We found that 19 out of 20 organisations had a security policy, and 16 of 20 organisations had an approved policy for handling of security incidents. This gives the impression that everything regarding security incident handling is taken care of. Further studies of the answers tell us that there are still many organisations that lack good implementation of the policies.

We have found in our survey that there is a difference in how private and public organisations handle their security incidents. We have described earlier in this chapter some reasons why this difference occurs. In this master thesis, we also wanted to see how different organisations defined security incidents. 80% of the organisations have defined what a security incident is and listed what they believe to be the most common incidents (see Table 8).

We also asked at what level the organisations were capable of detecting security incidents. We found here that the organisations did not to a large extent trust their organisations capability to detect all security incidents. This also compares with the question asking if the organisations thought that they ever could get a total overview over security incidents. The majority of the organisations did not believe that it was possible to get a total overview over all security incidents. There was, however, also a majority who believed that a good security incident handling would increase the security level in their organisation.

As mentioned before, training is a considerable factor that contributes to getting a better handling of security incidents. Exercises are also a measure that has to be used to get the organisation and the employees to improve. We asked the organisation some questions regarding effect of training. This would again give us better understanding of one of our research questions. The majority of the private organisations answer that training to a large extent gives positive effect on reported security incidents, increased focus on security incidents and better management support for security work. The majority of the public organisations answer here that it to some extent has positive effect on reported security incidents, increased focus on security incidents and better management support for security work. Overall understanding of these results tells us that training is seen as giving positive effects on handling of security incidents.

In earlier surveys [8] regarding the number of security incidents, it has been pointed out that the attained numbers can be somewhat underreported. Reasons for this can be many, but this information is still seen as classified and sensitive or information that can give bad reputation or tempt hackers to attack their systems. We have in our survey asked for reported security incident in 2004 and how many incidents were notified to the police. One interesting finding here was that 40% of the organisations did not know how many incidents were reported and that 35% of the organisations answered between 0-24 incidents reported. This indicates that the organisations either do not know the actual number of incidents or that there is a breach in the implementation of the incident handling routines. Only two organisations answered that they had over 100 incidents reported. From our perspective, this shows that there is a mismatch between published material regarding security incidents and the numbers we found in our survey. "Mørketallsundersøkelsen 2003" [37] shows that Norwegian companies have been exposed to:

- 5200 data break-inn's
- 2,7 mill. attempts of data break-inn's
- 150 000 virus infections
- 50 mill. attempts of virus infections

This survey also shows that over 50% of the organisations in 2003 did not have routines for security incident reporting. Our survey shows that 80% have such routines. When we studied the numbers of incidents reported to the police this corresponded with [37]. 187 computer crimes were notified to the police in 2003. Our survey found that only a few organisations notified incidents to the police. The total number of incidents notified to the police was 12. 1 organisation had policy against answering this type of question.

When we analyze all responders' answers it seems that the handling of security incidents especially in the private sector is well documented and that both training and routines are in place. When we go into more detail and analyze the handling in Section 5.2.2, we find that the level in some parts of the incident handling could have been better, especially in the public domain. Areas to mention are to have:

- Ability to detect security incidents
- Ability to report security incidents
- Good statistics over security incidents.

Regarding reporting security incidents, we asked how security incidents were reported, to which role and in what way – matrix structure or tree structure. In our opinion, it is of major interest to find out if one or another reporting structure is better than the other. To find the best reporting structure could give the organisations great benefits when deciding how to set up a security incident handling system. This topic is further described in Chapter 8.

7 Conclusion

To be able to handle security incidents in the most effective way, it is very important to both have a well functioning reporting system and have trained employees. This master thesis shows that there are many theoretical approaches to how to deal with security incidents and best practices are described. To find a way of taking this theory into a practical implementation seems however difficult. We have seen that many organisations have policies and routines, but when it comes to how each employee both knows what a security incident is and where to report the incident and who is going to act, there is still room for improvements. The statistical material about security incidents that the organisations are exposed to is in many cases not existent or the data cannot be trusted. The most common reasons for this are lack of implemented routines, lack of training, and that the organisations have not defined what a security incident is.

We found that surprisingly many private organisations say that they have both routines and training in place. The same private organisations have also to a large extent reporting systems in place. They have also to a large extent a handling point for security incidents.

The public organisations in our survey still have a way to go in order to reach the expected level of security incident handling. Only a few public organisations can achieve the level that the private organisations have set. We have found that few public organisations can match the level of the private organisations. Those who can are found within the health service domain. The rest of the public organisations lack both training, incident handling policies, security incident definitions and statistic material about how many security incidents they are exposed to.

Many organisations now outsource their IT-systems and surveys show that in many cases there are no documented routines for security incident handling between the two parties. By introducing security metrics, we have shown that both in outsourcing deals and in the very organisation these metrics can improve security work.

To some extent the organisations are capable of discovering security incidents. There must, however, be an increased focus on the topic and an increased focus on training and exercise about handling security incidents. In this way, the organisations can be prepared when a security incident occurs.

As indicated in the title of this master thesis: “Security incident handling and reporting – a study of the difference between theory and practice”, we can conclude that it still is a difference between theory and practice regarding how organisations handles security incidents.

8 Further work

8.1 Modelling Network structure

The survey has shown us that most of the organisations report in a tree structure, meaning that the person/system that detects a security incident reports the incident to a person/role into a defined chain. To find out which reporting structure is the best it would be of great interest to find a method to measure different ways of reporting security incidents. In this chapter, we give examples on how this can be done. To accomplish this, we have to model a network in order to measure the efficiency of different reporting structures. In order to do this, we could start from the way in which a large company reports security incidents. The model could start with an organisation that reports incidents in a tree-structure, i.e the security incidents are reported to defined persons in a hierarchy. The main structure of our model could be as follows:

The organisation consists of three business units and has a corporate level on top. Each business unit has its own Computer Security Incident Response Team (CSIRT) with a defined reporting chain. In the business units there are 20-40 different ICT systems, with defined system owners. In this example, we have not taken into consideration the automated incident handling, i.e. from Intrusion detection systems, firewall logs, etc. but have modeled the human part of the reporting structure. In the modeled company each employee has responsibility to report security incidents to their nearest superior or to the helpdesk. The nearest superior then reports the security incident to the business unit CSIRT. The Business unit CSIRT can take action or let the corporate CSIRT have the responsibility. In some cases, the problem can also be given to the operations department, which runs the system that is affected. In the model, we assume that the solving point is the CSIRT team either in the business unit or at the corporate level. We also assume that security incidents are defined and that the employees are trained in handling security incidents.

8.1.1 The network

The communication capacity of the modelled network is assumed not to be a problem. The capacity of nodes in the network is seen as the week link in the reporting chain. By using a mathematical approach to this model, it could be possible to calculate node capacity, network capacity, CSIRT capacity and other elements that can give the effectiveness of different reporting structures. One example could be to find if a tree structure reporting chain is more effective than reporting into a matrix structure.

8.2 Mapping of tools and methods

One of the challenges for private and public organisations is knowing which products are available on the market pertaining to security incident handling and reporting. One relevant research question here could be:

- What types of software and methodology exist for security incident handling and reporting?

This is a question that can be studied so that organisations could get an overview of the product market. One approach could be to locate such products and carry out telephone interviews with selected suppliers. By using qualitative methods in the interviews it is possible to get an overview of the scope of these products as well as a simple evaluation of the products' user friendliness and efficiency.

8.3 Other work

When more organisations have established policies and implemented routines for handling security incidents, hopefully according to the reporting structure described here and by following our checklist, a new survey can be carried out.

9 References

[1] Per Arne Enstad. ”Når hellet er ute må vi som minimum forsøke å minimalisere de negative konsekvensene”. Uninett konferansen 13 juni 2002. Electronical version on: http://www.hisf.no/uninett2002/foredrag/torsdag/MinimalisereUhell-Uninett-Ernstad.pdf

[2] John D. Howard, Thomas A. Longstaff “A Common Language for Computer Security Incidents”. Electronical version on: http://www.cert.org/research/taxonomy_988667.pdf

[3] Ernst&Young publikasjon 2004 ”Risikostyring innen informasjonssikkerhet” . Electronical version on: http://www.ey.com/global/download.nsf/Norway/TSRS_Mer_om_informasjonssikkerhet/$file/Mer%20om%20informasjonssikkerhet.pdf

[4] CERT Coordination Centre publiserer statistikk over innrapporterte sikkerhetshendelser, Electronical version on: http://www.cert.org/stats/#incidents

[5] CERT Coordination Centre kommenterer 2004 E-Crime Watch Survey, 2004 eCrime watch survey conducted by CSO Magazine, CERT and Carnegie Mellon University Software Engineering Institute, Electronical version on: http://www.csoonline.com/releases/ecrimewatch04.pdf

[6] Richard L. Rollason-Reese, Incident handling: an orderly response to unexpected events. September 2003 Proceedings of the 31st annual ACM SIGUCCS conference on User services. Electronical version on: http://delivery.acm.org/10.1145/950000/947496/p97-rollason-reese.pdf?key1=947496&key2=9123308901&coll=GUIDE&dl=GUIDE&CFID=29277858&CFTOKEN=98567137

[7] John P. Wack, Establishing a Computer Security Incident Response Capability (CSIRC). Electronical version on: http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf

[8] "CERT® /CC Statistics 1988-2003." Carnegie Mellon University Software Engineering Institute, CERT Coordination Center Juli 2003. Electronical version on: www.cert.org/stats/

[9] Thomas A. Longstaff. Special Report CMU/SEI-93-SR-20. “Results of a Workshop on Research in Incident Handling September 1993”. Electronical version on: http://www.sei.cmu.edu/pub/documents/93.reports/pdf/sr20.93.pdf

[10] Knut Helge Vindheim. ”Intrusion Detection og aktiv søking etter sikkerhetsrelaterte hendelser”. Electronical version on: http://www.hisf.no/uninett2002/foredrag/torsdag/InturisionDetection-NTNU-Vindheim.pdf

[11] Killcrece, Kossakowski, Ruefle, Zajicek (2003): “State of the Practice of

Computer Incident Response Teams (CSIRTs)", Technical Report CMU/SEI-2003-TR-001, Pittsburgh PA, Networked Systems Survivability Program, Software Engineering Institute, Carnegie Mellon University

[12] BS ISO/IEC 17799. "Information technology - Code of practice for information security management", BS ISO/IEC, 2000.

[13] BS 7799-2. "Information security management systems - Specification with guidance for use". BS, 2002.

[14] West-Brown, Stikvoort, Kossakowski, Killcrece, Ruefle, Zajicek (2003): "Handbook for Computer Security Incident Response Teams (CSIRTs)" 2nd edition, Handbook CMU/SEI-2003-HB-002, Pittsburgh PA, Networked Systems Survivability Program, Software Engineering Institute, Carnegie Mellon University

[15] Brownlee, Guttman (1998): Request For Comments 2350, Expectations for Computer Security Incident Response, Electronical version on: http://www/.ietf.org/rfc/rfc2350.txt

[16] Tim Grance, Karen Kent, Brian Kim. „Computer Security Incident Handling Guide" Recommendations of the National Institute of Standards and Technology NIST800-61. Electronical version on: http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

[17] Klaus-Peter Kossakowski. "Bibliography of Computer Security Incident Handling Documents". Electronical version on: http://www.dfn-cert.de/eng/pre99papers/certbib.html#[Schultz%20Jr.%20et%20al.%201990

[18] "Telenors prosjektstyringsmodell", Limited access on demand.

[19] Haug, Tor Grude, Kristoffer V. Andersen, Erling S. "Målrettet prosjektstyring" ISBN 8256260645

[20] "Telenors risikoanalyseverktøy". Limited access on demand

[21] Norwegian standard: Risikoanalyse NS 5814. 1991. Norges standardiseringsforbund (NSF)

[22] www.kins.no

[23] www.securityforum.org

[24] Frode Volden, Gjøvik University College, "lecture notes from Scientific methodes 2004"

[25] Shirley Payne, "A guide to security metrics" July 11 2001, www.sans.org/rr/papers/5/55.pdf

[26] Bakås, Orderløkken, Hagen. Gjøvik University College 2003. "Security Metrics for outsourcing operational services"

[27] Norges Standardiseringsforbund (The Norwegian Standards Association) "NS-ISO/IEC 17799", May 2001

[28] Einar Snekkenes, Gjøvik University College "Lecture notes for a course on security metrics, 2003"

[29] http//scrc.nist.gov/csspab/june13-15/jelen.pdf

[30] Swanson, Bartol, Sabato, Hash, Graffo, "Security Metricz Guide for Information Technology Systems", NIST, July 2003]

[31] Orderløkken, Tore Larsen "Forprosjektplan 2004" Høgskolen i Gjøvik

[32] John W. Creswell, Research Design: "Qualitative, Quantitative, and Mixed Methods Approaches"

[33] The Oxford Reference Dictionary; Oxford University Press, 1986

[34] Longman Dictionairy of Contemporary English Online; www.idoceonline.com

[35] R Shirey, "Internet Security Glossar", RFC2828 May 2000

[36] Federal Office for Information Security (BSI) "IT Baseline Protection Manual" www.bsi.bund.de

[37] Mørketallsundersøkelsen 2003 http://www.nsr-org.no/docs/79281401M.pdf

APPENDIX A.

Checklist for security incident handling

This checklist is made as an example of how an organisation can start a security incident handling program. This checklist gives a prioritized set of actions that has to be taken into consideration if the organisation wants to succeed with their security incident handling implementation. This checklist is based on the author's own experience, inputs from the survey and is based on the best practices given in Chapter 2.

Security incident handling steps:

Security Incident handling should be divided into phases starting with the preparation phase. The next phases consist of identification, containment, eradiction, recovery and follow up. Each phase has in our example been divided into steps as shown in Table 15.

There are some things one wants to avoid when dealing with incidents. That is ignorance, no decision-making, no response when reporting incidents, and no action taken even if the incident also affects other units in the organisation. Another thing that has also to be taken into account is how consequences will be used if our own employee has caused the incident to happen.

Security incident handling - implementation checklist.

Security incident handling - implementation checklist		
STEPS	ACTION	Checked
Phase 1: Preparation (Policy and decision-making).		
1.1	Establish a security policy	
1.2	Get management support for starting a security incident handling program	
1.3	Establish a security incident handling policy	
1.4	Define what types of security incidents can affect the organisation and to what extent	
1.5	Establish an organisation for handling incidents	
1.6	Start training within the established organisation	
1.7	Establish a communication plan for security incident handling (include who to notify both internally and externally, and provide information to system owners, administrators and users how incident handling is organised)	
Phase 2: Identification (determine if an incident has occurred or not, determine the nature of the incident).		
2.1	Has an incident occurred, what type, assign a person to be responsible for the incident	
2.2	Coordinate with operating units and system owners	
2.3	Notify supervisors or managers, operating units, IT security officer, IT department	
2.4	Make an escalation strategy	
Phase 3: Containment (Limit the scope and magnitude of the incident so that it is not getting worse).		
3.1	Deploy Computer Incident Response Team or other groups on-site to start working	
3.2	Back up the system (e.g. to acquire evidence)	
3.3	Do risk assessments whether to stop or continue operations	
Phase 4: Eradiction (Ensure that the problem is eliminated)		
4.1	Isolation of the attack, how was it executed	
4.2	Implement security measures to avoid similar situation in the whole organisation	

4.3	Perform vulnerability tests	
4.4	Remove the cause of the incident	
Phase 5: Recovery (Get the affected system back to the fully operational status).		
5.1	Restore the system (decide when)	
5.2	Validate system after restoring	
5.3	Monitor for backdoors or other things that might not have been detected	
Phase 6: Follow up (Lessons learned to avoid future incidents)		
6.1	Incident report sent to address list stated in the policy	
6.2	Recommend changes both to the policy and the system	
6.3	Implement changes	

Table 15 Incident handling checklist.

APPENDIX B.

Questionnaire cover letter (in Norwegian)

SPØRREUNDERSØKELSE VEDRØRENDE HÅNDTERING OG RAPPORTERING AV SIKKERHETSHENDELSER

Lillehammer 18 februar 2005

Håndtering av sikkerhetshendelser og sikkerhetsbrudd er en viktig del av sikkerhetsarbeidet i enhver organisasjon. Gjentatte og/eller alvorlige sikkerhetshendelser kan føre til sikkerhetsbrudd som må håndteres. Hvis man kan gi ledelsen en status og statistikk på hvilke sikkerhetshendelser og sikkerhetsbrudd man er utsatt for, kan man få økt fokus på sikkerhetsarbeidet.

Mitt navn er Tore Larsen Orderløkken og jeg studerer informasjonssikkerhet ved Høgskolen i Gjøvik (HIG), i tillegg arbeider jeg i Telenor som leder for Kompetansesenter Informasjonssikkerhet. Jeg er nå i ferd med å skrive en Masteroppgave som avslutning på mitt studie ved HIG. Tittelen på oppgaven er:

”HÅNDTERING OG RAPPORTERING AV SIKKERHETSHENDELSER – EN STUDIE AV FORSKJELLEN MELLOM TEORI OG PRAKSIS”.

For å få et best mulig resultat er jeg avhengig av å gjennomføre en spørreundersøkelse blant private og offentlige organisasjoner. Dette for å kunne si noe om hvordan sikkerhetshendelser blir håndtert og rapportert. Det er i denne forbindelse jeg nå henvender meg til dere.

På de neste sidene finner dere en spørreundersøkelse. Mitt ønske er at dere tar dere tid til å besvare undersøkelsen slik at jeg får et godt underlagsmateriale for min Masteroppgave. **All informasjon som kommer inn vil bli konfidensialitetsbeskyttet, og i oppgaven vil alle data bli anonymisert.**

Dere vil som takk for hjelpen få tilsendt den ferdige Masteroppgaven, forhåpentligvis vil den være et verdifullt bidrag i deres egen organisasjons arbeid med sikkerhetshendelser.

Hvis det ikke er ønskelig å delta i et slik arbeid gi meg en tilbakemelding. Hvis det er andre i din organisasjon som bør svare på dette, send videre og gi meg beskjed slik at jeg kan få korrigert min adresseliste.

På forhånd takk

Vennligst returner spørreskjemaet innen torsdag 10 mars 2005 ved :

- Epost: tore-larsen.orderløkken@telenor.com
- Post til: Tore Larsen Orderløkken Kirkegt. 45 2609 Lillehammer.

Med vennlig hilsen
Tore Larsen Orderløkken
Telefon: 907 30 675

APPENDIX C.

Questionnaire sent to organisations (in Norwegian)

I dette spørreskjemaet skal du i hovedsak sette kryss i den rubrikk du mener er riktig. I noen spørsmål skal du svare skriftlig.

1 POLICY - RUTINER

Spørsmål		Ja	Nei
1.	Har din organisasjon en sikkerhetspolicy?		
2.	Inkluderer sikkerhetspolicyen informasjonssikkerhet/IT-sikkerhet?		
3.	Hvem har godkjent organisasjonens sikkerhetspolicy?	Kryss av	
		Ledelsen	
		Sikkerhetssjef	
		Avdelingssjef	
		Ingen	
		Andre	
4.	Følger din organisasjon en standard for informasjonssikkerhet *(eks BS7799, ISO17799, ISF Standard of Good Practice etc)?*	Ja	Nei
5.	Har din organisasjon en godkjent policy/rutine for håndtering og rapportering av sikkerhetshendelser?		
6.	Har din organisasjon definert hva som er en sikkerhetshendelse?		
7.	Er det i din organisasjon et mottaksapparat for rapporterte sikkerhetshendelser *(eks Tigerteam, Computer Incident Responce team (CIRT), IT-avd, sikkerhetssjef etc)?*		
8.	Har din organisasjon en form for ”whistle blowing”/anonym rapportering av sikkerhetshendelser?		
9.	Lages det i din organisasjon statistikk/regnskap over antall sikkerhetshendelser?		
10	Skiller dere mellom sikkerhetshendelser og sikkerhetsbrudd?		
11	Utfyllende tekst/Kommentarer (vennligst spesifiser):		

2 PRAKTISK HÅNDTERING AV SIKKERHETSHENDELSER

Ut fra din kunnskap til egen organisasjon - i hvor stor grad er:		I liten grad				I stor grad	Vet ikke
		1	2	3	4	5	
12	- din organisasjon i stand til å oppdage sikkerhetshendelser						

13	- din organisasjon i stand til å rapportere sikkerhetshendelser						
14	- din organisasjon i stand til å reagere på sikkerhetshendelser						
15	- din organisasjon klar over hvilke trusler man står ovenfor innen informasjonssikkerhets området						
16	- din organisasjon risikostyrt (dvs at avgjørelser tas på bakgrunn av risikovurderinger)						

3 DEFINISJON AV SIKKERHETSHENDELSER

For å få en oversikt over hva den enkelte organisasjon legger i ordet sikkerhetshendelse ber jeg om at dere ut fra egen organisasjons definisjoner eller fra eget ståsted angir inntill 10 sikkerhetshendelser.		
17	Sikkerhetshendelser	Angi Hendelse (eks Denial of Service, Virusangrep, brudd på sikkerhetspolicy etc)
	Sikkerhetshendelse 1	
	Sikkerhetshendelse 2	
	Sikkerhetshendelse 3	
	Sikkerhetshendelse 4	
	Sikkerhetshendelse 5	
	Sikkerhetshendelse 6	
	Sikkerhetshendelse 7	
	Sikkerhetshendelse 8	
	Sikkerhetshendelse 9	
	Sikkerhetshendelse 10	

4 OPPFØLGING AV SIKKERHETSHENDELSER

18	Har din organisasjon verktøy for håndtering og rapportering av sikkerhetshendelser og sikkerhetsbrudd?		Ja	Nei
	Hvis ja hvilken type verktøy?		▨	▨
	17 a	Kommersielle?		
	17 b	Hvis kommersielt, fra hvilken leverandør?		
	17 c	Egenutviklede?		
19	Til hvem skal sikkerhetshendelser rapporteres i din organisasjon?		Kryss av:--	
			Ledelsen	
			Sikkerhetssjef	
			Egendefinert rapporteringsenhet	
			Nærmeste leder	
			Andre (spesifiser):	
20	Rapporteres sikkerhetshendelser inn i en tre-struktur dvs at den som oppdager hendelsen rapporterer til neste person i en definert kjede?		Ja	Nei

21	Rapporteres sikkerhetshendelser inn i en matriseorganisasjon? dvs at det er flere veier å rapportere om en sikkerhetshendelse.		
22	Er kapasitet på behandling av sikkerhetshendelser et tema i din organisasjon?		
23	Hvor mange sikkerhetshendelser/sikkerhetsbrudd ble rapportert i din organisasjon i 2004?		Kryss av: --
		0 – 24	
		25 – 49	
		50 – 99	
		Over 100	
		Vet ikke	
24	Hvor mange sikkerhetshendelser/sikkerhetsbrudd ble anmeldt		Spesifiser:--
		Antall	
		Vet ikke	
25	Utfyllende tekst/Kommentarer (vennligst spesifiser):		

5 OPPLÆRING

Har de ansatte fått opplæring i:		Ja	Nei
26.	Hva som er en sikkerhetshendelse?		
27.	Hva de skal gjøre hvis de oppdager en sikkerhetshendelse?		
28.	Hvor sikkerhetshendelser skal rapporteres?		

Uavhengig av om det er gitt opplæring eller ikke, i hvor stor grad er:		I liten grad				I stor grad	Vet ikke
29.	- de ansatte i din organisasjon kjent med hvordan de skal håndtere sikkerhetshendelser?						
30.	- hvor de skal finne informasjon om håndtering av sikkerhetshendelser?						
31.	- hvor de skal rapportere sikkerhetshendelser?						
Hvis det er gitt opplæring, i hvor stor grad gir det:		I liten grad				I stor grad	Vet ikke
32.	- en merkbar effekt på antall rapporterte sikkerhetshendelser?						
33.	- økt fokus på sikkerhetshendelser?						
34.	- bedre ledelsesstøtte/forankring for sikkerhetsarbeid?						

6 Sikkerhtshendelseshåndtering og dens innvirkning

Hvordan vekter du følgende utsagn? (Sett kryss)

Bruk **1 for ikke riktig**
6 for helt riktig

Gradering		1	2	3	4	5	6
35.	Alle ansatte i min organisasjon kjenner til hva som er sikkerhetshendelser.						
36.	Alle ansatte i min organisasjon vet hvor de skal rapportere						

	sikkerhetshendelser.						
37.	Vi er i stand til å detektere sikkerhetshendelser.						
38.	Det er lettere å få gjennomslag for sikkerhetsinvesteringer hvis vi har oversikt over sikkerhetshendelser.						
39.	Vil en god sikkerhetshendelseshåndtering øke sikkerhetsnivået i egen organisasjon						
40.	Hvis vi har oversikt over sikkerhetshendelser vil vi kunne sette inn tiltak på en mer effektiv måte.						
41.	Du vil aldri få en total oversikt over sikkerhetshendelser og sikkerhetsbrudd?						
42.	Det er ingen kultur i min organisasjon for å rapportere sikkerhetshendelser?						
43.	Man kan selv bli mistenkeliggjort når man rapporterer sikkerhetshendelser?						
44.	Jeg vil aldri rapportere sikkerhetsbrudd som kolleger har begått?						

7 Om deg og din organisasjon.

Stilling		Fyll ut	
45	Hva er din stilling i organisasjonen?		
46	Hvilken rolle i organisasjonen rapporterer du til?		
47	Hvor mange ansatte er det i din organisasjon?	0 –199	
48		200 – 999	
49		1000 - 4999	
50		Over 5000	

51.	Hvilken sektor tilhører din virksomhet?		
1. Bank, finans, forsikring		7. Offentlig sektor	
2. Kjemikalier, helse		8. Detaljhandel	
3. Energi, kraft		9. Leverandør av IT tjenester	
4. Industri/ produksjon		10. Telekommunikasjon	
5. Media, post		11. Transport	
6. Prosessindustri		12. Annet (vennligst spesifiser):	

Har du andre/utfyllende kommentarer til håndtering og rapportering av sikkerhetshendelser, bruk dette feltet.	
Hvis du ønsker å få resultatet av undersøkelsen, vennligst fyll inn følgende felter:	
Navn på virksomhet:	Navn:
Telefonnummer:	E-post:

Tusen takk for at du fylte ut spørreskjemaet.

Vær vennlig og returner skjemaet i utfylt stand **innen torsdag 10. mars 2005 til:** **tore-larsen.orderløkken@telenor.com** eller med vanlig post til Tore Larsen Orderløkken, Kirkegata 52 2609 Lillehammer.

APPENDIX D.

Survey/Questionnaire results

In this appendix we outline the answers given from the participants in the survey with statistics and short comments.

Part 1: Policy and routines

Question 1: Does your Organisation have a security policy?

95% of the organisations answered that they have a security policy.

100% of the private and 90,1% of the public organisations have a security policy.

Question 2: Does your security policy include information security/IT-security?

95% of the organisations answered that they have included information security into their security policy.

100% of the private and 90,1% of the public organisations have included information security in their security policy.

Question 3: Who has approved your organisation's security policy?

90% answer that top management has approved the organisation's security policy and 10% of the organisations answered that no one has approved the policy.

No private organisations and 18,2% of the public organisations answer that they have no approved policy.

Question 4: Does your organisation follow a standard for information security (i.e. BS7799, ISO17799, ISF standard of good practice etc)?

50% answer that they follow an international standard and 47,4% answer that they do not follow any international standard.

88,9% of the private organisations follow a standard but only 18,2% of the public organisations follow a standard for information security.

Question 5: Does Your Organisation have an approved policy for handling and reporting of security incidents?

80% answer that they have an approved policy, 20% that they do not have an approved policy for handling and reporting security incidents.

88,9% of the private organisations have an approved policy for handling and reporting of security incidents and 72,7% of the public organisations have an approved policy for handling and reporting of security incidents.

Question 6: Has Your Organisation defined what a security incident is?

80% of the organisations have defined security incidents, 20% have not defined what a security incident is.

88,9% of the private organisations and 72,7% of the public organisations have definitions.

Question 7: Is there in your organisation a defined handling point for security incidents (e.g. Tiger Team, Computer Incident Response Team (CIRT), IT-Department, security manager etc.)?

70% of the organisations have a defined handling point, 30% have not.

88,9% of the private organisations and 54,5% of the public organisations have a defined handling point.

Question 8: Has Your Organisation some form of ”whistle blowing” or anonymous reporting of security incidents?

75% of the organisations have no form of whistle blowing or anonymous reporting of security incidents.

77,8% of the private and 72,7% of the public organisations have no such systems.

Question 9: Has your Organisation made any statistics/accounts over the number of security incidents?

60% of the organisations make statistics over the number of security incidents and 36,8% do not.

77,8% of the private organisations and 45,5% of the public organisations make statistics.

Question 10: Does your organisation distinguish between security incidents and security breaches?

45% of the organisations make distinguishes between security incidents and security breaches and 55% do not.

77,8% of the private organisations and 18,2% of the public organisations make a distinction between the two.

Question 11: Room for comments:

No significant comments.

Part 2: Handling of security incidents in practice

Question 12: From your knowledge in your own organisation, to what extent is:

(Grading 1-5 where 1 corresponds to "to a little extent" and 5 corresponds to "to a large extent". To get the data from these questions, we have classified the data into three categories. The answers in scale 1-2, scale 3 and scale 4-5 have been calculated).

- Your organisation capable of discovering security incidents?

20% of the organisations grade this in the lower end of the scale (1-2). That means they answer that they discover security incidents to a little extent. 35% grades this in the middle of the scale (3), and 45% in the upper level of the scale (4-5) meaning that they discover security incidents to a large extent.

36,4% of the public organisations and 0% of the private organisations are in the lower end of the scale meaning that they discover security incidents to a little extent.

77,8% of the private organisations and 18,2% of the public organisations are in the high end of the scale (4-5) meaning that they discover security incidents to a large extent.

Question 13: - Your organisation capable of reporting security incidents?

20% of the organisations grade this in the lower end of the scale (1-2) meaning that their organisation is capable of reporting security incidents to a little extent. 35% of the organisations grade this in the middle of the scale (3) and 45% in the area 4-5 meaning that they think their organisations is capable of reporting security incidents to a large extent.

36,4% of the public and 0% of the private organisations are in the lower end of the scale (1-2) meaning that their organisations are capable of reporting security incidents to a little extent.

54,5% of the public and 11,1% of the private organisations are in the middle of the scale (3).

9,1% of the public and 88,9% of the private organisations are in the high end of the scale (4-5) meaning that their organisations report security incidents to a large extent.

Question 14: - Your organisation capable of reacting on security incidents?

80% of the organisations answer that they are in the upper end of the scale (grading 4-5) meaning that they can react on security incidents to a large extent.

63,6% of the public and 100% of the private organisations are in the upper end of the scale.

27,3% of the public and 0% of the private organisations are in the lower end of the scale (1-2) meaning that they are capable of reacting on security incidents to a little extent.

Question 15: - Your organisation realize the threats you are facing within the information security area?

70% of the organisations answer that they are in the upper end of the scale (grading 4-5) meaning that they are realizing the threats they are facing to a large extent. Only 5% answers that they are realizing threats (grading 1-2) to a little extent. 25% of the organisations answer that they realize the threats to some extent.

54,6% of the public organisations and 88,9% of the private organisations answer that they are in the upper end of the scale (4-5) meaning that they are realizing the threats they are facing to a large extent. No Private organisations are in the lower end of the scale but 9,1% of the public organisations are in the lower end of the scale meaning that they realize the threats they are facing to a little extent.

Question 16: - Your organisation risk managed (i.e that decisions are taken based on risk assesements).

25% of the organisations answer that they are risk managed (1-2 on the scale) to a little extent. 25% of the organisations answer that they are risk managed to some extent. 50% of the organisations answer that they take decisions based on risk assessments to a large extent.

36,4% of the public and 11,1% of the private organisations answer that they are risk managed (1-2 on the scale) to a little extent. 27,3% of the public and 22,2% of the private organisations answer that they are risk managed to some extent. 36,4% of the public and 66,7% of the private organisations answer that they are risk managed to a large extent and thereby take decisions based on risk assessments.

Part 3: Definitions of security incidents

Question 17: From your own organisation's definitions or from your own experience, point out 10 examples of security incidents.

14 organisations answered this question. Many of them gave almost the same definitions. In Table 16 Security Incidents definitions we have listed some of the most used definitions.

Table 16 Security Incidents definitions

Security Incidents defined by the organisations:
Virus attacks
Hacking
Breach of policy, regulations and laws
Loss of sensitive or classified information
Illegal downloading
DoS/DDOS attacks
Misuse of IT equipment
Deactivated security mechanisms
Fire
Theft
Lending out username and password
Sending sensitive/classified e-mail to unauthorised recipients
Unauthorised security scanning
Phishing
Threats against organisation or staff
Human errors
Fraud
Unauthorised use
Power failure
Unauthorised tunnelling through firewall
Breach of professional secrecy

There were no big differences between public and private organisations in this matter. The same definitions are used in both organisations.

Part 4: Follow-up of security incidents

Question 18: Has your organisations tools for handling and reporting security incidents and security violations?

55% of the organisations have tools for handling and reporting security incidents. 45% have no tools for handling and reporting security incidents.

45,5% of the public and 66,7% of the private organisations have tools for handling and reporting security incidents.

There are different vendors and different systems in place in the organisations which answer that they have tools. Remedy, Action request, Service desk, TQM Partner and some self-made systems are in use.

Question 19: To whom in your organisation will security incidents be reported?

On this question, 40% of the organisations answered that they report to one role in the organisation. The role they report to differs between management, security manager and the closest superior.

55% of the organisations report security incidents to different roles in their organisation. There are from 2-4 different reporting points in each organisation.

5% answer that they do not report to any point/role in the organisation.

Question 20: Are security incidents being reported into a tree structure i.e. there is one reporting point in a hierarchy?

60% of the organisations report into a tree structure, meaning that the person reporting the incident reports to a person in a defined chain.

55,6% of the private and 63,6% of the public organisations report into a tree structure.

Question 21: Are security incidents being reported into a matrix structure i.e there are several ways to report security incidents.

55% of the organisations report into a matrix structure.

77,8% of the private and 36,4% of the public organisations report into a matrix structure.

We can also see from the answers to the question 20 and 21 that 27,3% of the public and 11,1% of the private organisations do not report either into a tree structure or a matrix structure. We can also see that 35% of the organisations answer that they report both into a tree structure and a matrix structure.

topic

40% of the organisations answer that capacity is a topic in their organisation.

55,6% of the private and 27,3% of the public organisations think that capacity is a topic.

Question 23: How many security incidents were reported in your organisation in 2004?

35% of the organisations had 0-24 incidents reported.

No organisations reported between 25 and 49 incidents.

15% of the organisations had 50-99 incidents reported.

11,1% of the organisations had over 100 reported security incidents.

44,4% of the organisations did not know how many incidents were reported.

Question 24: How many security incidents were notified to the police?

26,3% of the organisations did not know how many security incidents were notified. 73,7% of the organisations knew that and the numbers of notifications were between 0-5.

Question 25: Room for comments:
No significant comments

Part 5: Training

Have your employees got training in:

Question 26: What a security incident is?

55% of the organisations have training in what a security incident is.

27,3% of the public and 88,9% of the private organisations have this employee training.

Question 27: What they will do if they discover a security incident?

75% of the organisations say that the employee knows what to do if they discover a security incident.

54,5% of the public and 100% of the private organisations say their employees know what to do if they discover a security incident.

Question 28: Where to report security incident?

75% of the organisations say that the employees know where to report security incident.

54,5% of the public and 100% of the private organisations say their employees know where to report.

Independently on if training has been given or not, to what extent are:

Question 29: - your employees aware of how to handle security incidents?
(Grading 1-5 where 1 correspond to "to a little extent" and 5 corresponds to "to a large extent".
To get the data from these questions we have classified the data into three categories. The answers in scales 1-2 (little extent), 3 (some extent) and 4-5 (large extent) have been calculated).

40% of the organisations say that the employees know how to handle security incidents to a little extent. (1-2 on the scale). 25% say that their employees know how to handle security incidents to some extent (3 on the scale) and 35% answer that their employees know how to handle security incidents to a large extent (4-5 on the scale).

54,5% of the public and 22,2% of the private organisations answer that their employees (1-2) are aware to a little extent of how to handle security incidents. 36,4% of the public and 11,1% of the private organisations answer that their employees (3) know to some extent how to handle security incidents. 9,1% of the public and 66,7% of the private organisations answer that their employees know to a large extent how to handle security incidents.

Question 30: - Where they can find information about handling of security incidents?

45% of the organisations answer that their employees know to a little extent where to find information (1-2 on the scale). 25% say that their employees know to some extent where to find the information (3 on the scale). 30% answer that their employees know to a large extent where to find information about how to handle security incidents.

63,6% of the public and 22,2% of the private organisations answer that their employees (1-2) know to a little extent where to find information about how to handle security incidents. 27,3% of the public and 22,2% of the private organisations answer that their employees (3) know to some extent where to find information about how to handle security incidents. 9,1% of the public and 55,6%

of the private organisations answer that their employees know to a large extent where to find information about how to handle security incidents.

Question 31: - Where they shall report security incidents

25% of the organisations answer that their employees (1-2) know to a little extent where to report security incidents. 35% of the organisations answer that their employees (3) know to some extent where to report security incidents. 40% of the organisations answer that their employees (4-5) know to a large extent where to report security incidents.

36,4% of the public and 11,1% of the private organisations answer that their employees (1-2) know to a little extent where to report security incidents. 45,4% of the public and 22,2% of the private organisations answer that their employees (3) know to some extent where to report security incidents. 18,2% of the public and 66,7% of the private organisations answer that their employees (4-5) know to a large extent where to report security incidents.

If education is given, to what extent gives that:

Question 32: - a significant effect on the number of reported security incidents.

65% of the organisations answered this question. 54,5% of the public and 77,8% of the private organisations answered.

15,4% of the organisations answering answered that it had an effect to a little extent (1-2), 30,8% answered that it had some effect on the number reported. 30,8% answered that it had large effect on the number reported and 23,1% of the organisations did not know if it had any effect.

0% of the public and 28,6% of the private organisations answer that it had an effect to a little extent (1-2). 66,7% of the public and 0% of the private organisations answer that it had some effect on the number reported. 33,3% of the public and 71,4% of the private organisations answered that it had a large effect (4-5) on the number of security incidents reported.

Question 33: - increased focus on security incidents.

65% of the organisations answered this question. 54,5% of the public and 77,8% of the private organisations answered.

15,4% of the organisations answered that it had increased the focus to a little extent (1-2). 23,1% answered that it had increased the focus to some extent (3).

46,2% of the organisations thought that it had increased the focus to a large extent. 15,4% answered that they did not know if the focus had increased.

16,7% of the public and 14,3% of the private organisations answer that it increased to a little extent (1-2) the focus on security incidents. 33,3% of the public and 14,3% of the private organisations answer that it had some effect on the focus. 50% of the public and 42,9% of the private organisations answered that it had a large effect (4-5) on the focus on security incidents.

Question 34: - better management support/anchoring for security work?

65% of the organisations answered this question. 54,5% of the public and 77,8% of the private organisations answered.

7,7% of the organisations meant that it gave better management support to a little extent (1-2). 23,1% answered that it gave better management support to some extent (3). 53,8% answered that it gave better management support for security work to a large extent (4-5). 15,4% of the organisations did not know if it gave better management support.

0% of the public and 14,3% of the private organisations answer that it gave better management support for security work to a little extent (1-2). 33,3% of the public and 14,3% of the private organisations answer that it had some effect on the management support. 66,7% of the public and 42,9% of the private organisations answered that it had a large effect (4-5) on better management support for security work.

Part 6: Handling of security incidents and its effect

How do you weight the following statements: Use 1 for “does not agree” and grade your answers up to 6 that means you “totally agree”.

Question 35: - All the employees in my organisation know what a security incident is.

45% of the organisations answer that they do not agree with this statement (answers 1-2 in the tickboxes). 50% answer that they agree to some extent (3-4 in the tickbox). 5% of the organisations totally agree (5-6 in the tickbox).

22,2% of the private and 63,6% of the public organisations say that their employees know to a little extent what a security incident is. 66,7% of the private and 36,4% of the public organisations say that they know to some extent. 0% of the public and 11,1% of the private organisations say that all their employees know what a security incident is.

Question 36: - All the employees in my organisation know where to report security incidents.

35% of the organisations answer that they do not agree with this statement (1-2 in the tickbox). 40% answer that they agree to some extent (3-4 in the tickbox). 25% totally agree with this statement.

22,2% of the private and 45,5% of the public organisations did not agree (1-2). 22,2% of the private and 54,5% of the public organisations agree to some extent (3-4) with the statement. 55,6% of the private and 0% of the public organisations totally agree with this statement (5-6).

Question 37: - We are capable of detecting security incidents

10 % of the organisations answer that they do not agree with this statement (1-2 in the tick box). 65% answer that they agree to some extent (3-4 in the tick box). 25% totally agree with this statement (5-6 in the tick box).

0% of the private and 18,2% of the public organisations answer that they do not agree with this statement (1-2 in the tick box). 44,4% of the private and 81,8% of the public organisations agree to some extent with the statement. 55,6% of the private and 0% of the public organisations totally agree with this statement.

Question 38: - It is easier to get acceptance for security investments if we have an overview of security incidents.

5% of the organisations answer that they do not agree with this statement (1-2 in the tick box). 30% answer that they agree to some extent (3-4 in the tick box). 60% totally agree with this statement (5-6 in the tick box).

0% of the private and 9,1% of the public organisations answer that they do not agree with this statement (1-2 in the tick box). 33,3% of the private and 27,3% of the public organisations agree to some extent with the statement. 66,7% of the private and 54,5% of the public organisations totally agree with this statement.

Question 39: - A good handling of security incidents will increase the security level in our organisation.

90% of the organisations totally agree with this statement (5-6 in the tick box). 10% answer that they agree to some extent (3-4 in the tick box). No organisations disagree with this statement (1-2 in the tick box).

77,8% of the private and 100% of the public organisations totally agree with this statement. 22,2% of the private and 0% of the public organisations agree to some extent with the statement. No organisations answer that they disagree to some extent with this statement (1-2 in the tick box).

Question 40: - If we would have an overview over security incidents we could enforce security measures more effectively.

70% of the organisations totally agree with this statement (5-6 in the tick box). 30% answer that they agree to some extent (3-4 in the tick box). No organisations answer that they disagree with this statement (1-2 in the tick box).

66,7% of the private and 72,7% of the public organisations totally agree with this statement. 33.3% of the private and 27,7% of the public organisations agree to some extent with the statement. No organisations answer that they disagree with this statement (1-2 in the tick box).

Question 41: - You will never get a total overview of security incidents and security violations.

60% totally agree with this statement (5-6 in the tick box). 30% answer that they agree to some extent (3-4 in the tick box). 10% of the organisations answer that they disagree with this statement (1-2 in the tick box).

55,6% of the private and 63,64% of the public organisations totally agree with this statement. 33,3% of the private and 27,3% of the public organisations agree to some extent with the statement. 11,1% of the private and 9,1% of the public organisations answer that they do not agree with this statement (1-2 in the tick box).

Question 42: - It is not a custom in my organisation to report security incidents.

45% of the organisations answer that they do not agree with this statement (1-2 in the tick box). 50% answer that they agree to some extent (3-4 in the tick box). 5% totally agree with this statement (5-6 in the tick box).

55,6% of the private and 36,4% of the public organisations answer that they do not agree with this statement (1-2 in the tick box). 33,3% of the private and 63,6% of the public organisations agree to some extent with the statement. 11,1% of the private and 0% of the public organisations totally agree with this statement.

Question 43: - You can throw suspicion on yourself when reporting security incidents.

65% of the organisations answer that they do not agree with this statement (1-2 in the tick box). 30% answers that they agree to some extent (3-4 in the tick box). 5% totally agree with this statement (5-6 in the tick box).

66,7% of the private and 63,6% of the public organisations answer that they do not agree with this statement (1-2 in the tick box). 22,2% of the private and 36,4% of the public organisations agree to some extent with the statement. 11,1% of the private and 0% of the public organisations totally agree with this statement.

Question 44: - I shall never report a security violation committed by a colleague.

90% of the organisations answer that they do not agree with this statement (1-2 in the tick box). 5% answer that they agree to some extent (3-4 in the tick box). 5% totally agree with this statement (5-6 in the tick box).

88,9% of the private and 90,1% of the public organisations answer that they do not agree with this statement (1-2 in the tick box). 0% of the private and 9,1% of the public organisations agree to some extent with the statement. 11,1% of the private and 0% of the public organisations totally agree with this statement.

Part 7: About you and your organisation

Question 45: - What is your role in the organisation?

The majority of the responders are security managers or IT security managers. The rest are security advisors or ICT advisors.

Question 46: - To what role in the organisation do you report?

The majority of the responders report to management functions such as security director, CEO or IT Director.

Question 47: - How many employees are there in your organisation?

Number of employees	Number of organisations
0 –199	1
200 – 999	4
1000 - 4999	3
Over 5000	12

Questions 48, 49 and 50 are not a part of the questionnaire.

Question 51: - What branch does your organisation belong to?

What branch does your organisation belong to?			
1. Bank, finance, insurance	2	7. Public sector	9
2. Chemicals, health	1	8. Retail trade	
3. Energy, power		9. IT supplier	2
4. Industry/ production		10. Telecommunication	1
5. Media, post	1	11. Transport	1
6. Process industry		12. Other (Please specify):	2