Incident Reporting Systems

Anders Reed-Mohn

Master's Thesis
Master of Science in Information Security
30 ECTS
Faculty of Computer Science and Media Technology
Gjøvik University College, 2007

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

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

Abstract

Systematic collection of safety incident / accident data has been common in many industries for decades. An equivalent effort has not been made in the area of information security, exclusive perhaps of highly specialized organizations with such needs.

The systematic collection of incident data allows scientific research and investigation into their causes, ultimately leading organizations to introduce more effective safeguards. Several authors have suggested that incident reporting systems should be used to collect information security incident data.

This project explores a System Dynamics model of a general incident reporting system, previously developed by other researchers, and discusse hpw it can be usefuk in information security. The model is also compared to how an existing organization collects incident data, to find out if the assumptions of the model mathces a real world example, in this case a health care institution.

The purpose of the developed model(s) is to help organizations in developing or improving incident reporting systems for information security, being an aid in evaluating their (planned or existing) procedures and tools. Whilst this might have had relevance to only a limited group of organizations in the past, when fewer worked with information security, we see today that any organization that works with information systems must also deal with information security in some degree. An organization does not need to grow very large before no individual can easily keep oversight of all its workings. Thus a need for structured management arises, just as much in information security as in other business processes.

Acknowledgements

I would like to thank my supervisor, Prof. Jose J. Gonzales[1] for the idea for this thesis, and for his help and advice during the project. A large thank you also goes to doctoral student Finn Olav Sveen[2] for a lot of good advice, and for all his help on the interview questions. Thank you also to Eliot Rich at the University of Albany, for reviewing the interview protocol.

Oslo, October 31st 2007, Anders Reed-Mohn

[1] Prof. dr. techn., dr. rer. nat. Jose J. Gonzalez, Department of Computer Science and Media Technology, Gjøvik University College

[2] Departamento de Organicacion, Tecnun, Universidad de Navarra

Contents

List of Figures

List of Tables

1 Glossary

These are som key terms used in this paper:

Event	An attempted or unsuccesful breach of security
Incident	A successful breach of security

2 Introduction

Systematic collection of safety incident / accident data has been common in many industries for decades. An equivalent effort has not been made in the area of information security, but the need for this has been rapidly increasing over the last few decades. Businesses and other organizations have come to manage more and more information, and though the manual management of (largely paper based) information is complex in itself, the rapid introduction of ever more complex electronic information systems introduces even more complex challenges to information security.

Successful management of information security mandates effective business processes that take these challenges into consideration, and minimize risks and threat exposure. To develop (or improve) these business processes there must be a system or process for analyzing how existing processes meet the information security threats, allowing organizations to learn where there is a problem and to implement corrective actions.

This is where the information security incident reporting system (ISIRS) finds its place, enabling collection and analysis of incident data (over time), building knowledge to minimize or avoid future risk through organizational awareness and improved business processes.

2.1 Topics covered

The systematic collection of incident data allows scientific research and investigation into their causes, ultimately leading organizations to introduce more effective safeguards. Literature and research on incident reporting systems for information security is still somewhat scarce[1].

In finding a basis for an incident reporting process / system, we turn to the extensive research performed in safety science. This master's project analyzes a generic model for incident reporting (hereafter referred to as "the IRS model"), developed by other researchers. We have broken the model down to a set of hypotheses representing causal links between entities in the model, and discuss their implications and relevance for an ISIRS.

In collaboration with two other master's projects (see chapter 4) a common set of ten hypotheses were explored further through interviews with staff at organizations from different sectors (health care, defense, and energy). This paper discusses a health care case.

The results of the interviews were then analyzed to find clues as to the validity of applying safety science experiences to information security reporting, and whether the model is adequate for such a system.

[1] There are many commercial systems out there that relate to incident management and reporting, in a variety of forms. Consider, for instance, the multitude of systems that exist for IT Service management, which can all to some degree support incident reporting in general. However, we are looking for research targeted specifically at information security reporting.

2.2 Problem description

We claim that there is a growing need for information security management, and we devote some space to talking about how information technology has played a key role in this, and how the two are connected.

In a not too distant past, most information was still stored on paper, most processing of information was done manually. Copies of documents were generally made in manageable numbers, and it was even possible to identify one single original for a document. Information security threats to regular, civilian organisations included theft and unauthorized copying and use of information, physical loss of documents, verbal leaks, and (probably) to a certain extent, social engineering[2].

While the threats existed, they were to a certain extent controllable. Changes to physical copies were harder to make, and stealing a document meant that it had to be physically removed, if only temporary, or photographed / photocopied. All this takes some effort to do undetected, especially on a large scale.

Over the past 50 years (roughly), the use of electronic information systems has increased exponentially, and with it comes new challenges for protecting the information stored and used within these systems. In the beginning, data was mostly just processed in computers (hence the name), and data was stored in writing on paper. However, as computers grew in storage capacity and processing power, the computer industry created more complex systems that allowed for the storage of information in electronic form (the first commercially available hard disk came on the market in 1956[2]). This capability has opened up a can of worms, as far as information security goes. According to [3] businesses today increase their storage capacity by 30 to 50 percent per year. The amount of information we manage is not shrinking any time soon.

Where one previously would have a few, very tangible, paper copies of documents, we now have a multitude of electronic copies of documents. These can be read, processed and copied, even without the owner's knowledge, while the actual owner still holds the "original". Problems escalated further with the advent of networking. Copies of information can now be spread to most any corner of the world in a matter of milliseconds. If you are reading this thesis on a computer, you currently have at least two copies of this document. One copy is the document file (temporary or downloaded) that you now have on disk, the other is the copy in the working memory (RAM) of your computer[3].

Can you account for what all pieces of software on your computer might do with this document? Can you prove that no-one slipped a malicious, information stealing program into your computers memory? Do others have access to the same computer, maybe via a network so that you do not see what they are doing on the computer you share? Now think of just how much of our information handling is being done electronically today.

[2] Social engineering REFERENCE TO MITNICK, which originally pertains to the application of social science, seems to be regarded as the new kid on the block in information security. This is clearly a false view, since the "social engineer" is no different from the better known "con-man" that has existed for ages. The term con-man is said to be about 150 years old, and there are documented scams a hundre years older[1]. And the concept of fraud was likely not new then either.

[3] This has been shown to be a problem in itself: If you bought one copy of some software, are you in violation of the license agreement as soon as you load that software into memory?[4]

Not only is electronically stored information somewhat intangible, but the use of ever more powerful databases and data-correlation systems have made it easy to dig up vast amounts of information in a short time (which is what they are supposed to do). Unfortunately, it is just as quick to do for illegitimate purposes. Instead of having to steal a whole filing cabinet, someone looking for, let's say, social security numbers, now only have to copy the right database table in the right computer system.

Easy access is also a consequence of storing information in many places. Individuals' privacy protection is made harder by the fact that we now store our personal information so many places; health care institutions, government offices, credit card companies, and other organizations we have a relationship with, all usually store some personal information about us.

This is not a problem just for individuals, businesses give sensitive information to partners, contractors and government offices. Controlling the spread, use, and alteration of all this information is getting harder all the time.

The above gives some examples of how complex the handling of information has become, and also why *information* security and *information technology* (IT) security has become almost synonymous. In reality they are not, however, and the complexity of IT-security must not be allowed to overshadow other aspects of information security. Granted, information security today is a lot about IT-security, but we must not forget that good information security practices must take into account all three of People, Processes and Technology. Even if we could eliminate all information security threaths to our computers, at some point information will be accessed by humans, and transferred to their minds, print-outs or notepads.

Our information security defences must therefore be in line with how people and organizations work with information, also outside of their computers. We must also be able to adapt these defences in accordance with changing conditions in our organizations.

Since modern information systems creates many new vulnerabilities, or opportunities for security breaches, logically the number of security incidents will also rise. Knowing what incidents (could) occur, and learning to prevent or avoid them in the future is therefore a task of growing complexity. Using an incident reporting system for collecting and analyzing incident data could help organizations perform this task in an effective way, whether the incident takes place inside or outside our computers.

2.3 Motivation and benefits

As active information security management becomes more and more important, so does the need for proper management tools. The systematic collection of incident data allows scientific research and investigation into their causes[5], ultimately leading organizations to introduce more effective safeguards, and perhaps to business processes that are void of many vulnerabilities to begin with.

We seek then, to help organizations in developing or improving information security incident reporting systems (ISIRS) for information security, being an aid in evaluating their (planned or existing) procedures and tools. Whilst this might have had relevance to only a limited group of organizations in the past, when fewer worked with information security, we see today that any organization must deal with information security in some degree. An organization does not need to grow very large before no individual can easily keep oversight of all its workings. Thus a need for structured management arises, just as much in information security as in other business processes.

Before one can delve into the details of creating an ISIRS, one must have an understanding of how it will be put together, how it will work. Note that by "system" we are not referring to a computer system, but a complete process. This process encompasses electronic or manual information gathering, handling and processing, as well as analysis of results, and applications of those results in the organization, through personell training, business process improvements, or other feedback. Indeed, "incident reporting process" is just as good a term for what we mean. For analyzing the general structure of the ISIRS, working with a model allows us to examine, change and experiment with the systems functionality with complete freedom. Of course, for this to have real value, the model must be accurate enough to provide a realistic picture of how the system will behave.

To help attain this value, we examine the general model developed through others' research[5]. By looking into how well this IRS model maps to information security, we hope to produce pointers as to how organizations can use the model for building (or improving) their own ISIRS.

2.4 Research questions

In this paper we explore the use of an ISIRS for improving information security in an organization. We wish to know whether it (the ISIRS) is likely to be a fruitful investment, and whether the IRS model of [5] adequately describes such a system. To this end, we explore previous work on incident reporting in both safety science and information security. At the same time, we look specifically at the IRS model, which was based on studies of safety reporting systems. Since it is a very general model, it should be applicable in some degree to most information security incident reporting systems, and in this paper, we compare it to the incident reporting system of a health care institution.

Accordingly, we ask:

Question 1 *Can incident reporting be a useful tool for improving information security?*

Question 2 *Can the IRS model be used within information security?*

Question 3 *How does the IRS model correspond to a real life ISIRS?*

2.5 Structure of this report

To be added.

2.6 Terminology

Incidents and events. Abbreviations. Interchangeable terms.

To be added.

2.7 Confidenciality

Virtually all of the information gathered in this thesis is available in the public domain. Even from the the health care institution (a public hospital) we worked with, we have tried not to gather information that could not be publicised. We were given copies of internal security policies and regulations for review, and these documents were classified as non-sensitive. None of these are included in this report, though sections are referred to. However, during interviews, respondents have referred to situations where information security was found to be poor, or possibly compromised. Even if we do not describe *identifying details* of compromise here, we have still chosen not to reveal the name of the hospital, or the respondents.

3 Summary of claimed contributions

We believe this thesis shows how incident reporting can be an important tool for improving information security, contributing to improved knowledge and awareness in the whole of an organization. We present System Dynamics modelling as a valuable and practical way of designing and analyzing an ISIRS and its performance.

Lastly we show how an existing IRS model already provides a good basis for this, and how that model can fit into any organizations work to establish and maintain an ISIRS.

We hope that our findings can provide organizations with useful information on the application of incident reporting systems, perhaps inspiring them to consider implementing such processes themselves. And may those who already have such a system, find some support and useful references in their efforts to maintain and improve their system.

3.1 Scope and limitations

While the ISIRS is best described as a complete process covering not only incident data collection, but also feedback (to the organization) processes, personell training, and other organizational processes, this thesis does not go into details about these.

This would amount to evaluating several complex business processes and management areas, digging into fields far beyond information security. It is not within the scope, or time limits, of this thesis to do so. Instead we concentrate mainly on incident reporting in itself, and treat other areas, such as organizational learning, HR management etc, mostly as necessary "black boxes" in, or connected to, our ISIRS.

4 Choice of methods

Parts of this work has been coordinated with two other master's projects at HiG. The subject of the three theses is the same, but each approach to theory, discussions, analysis and case study is individual. The collaboration was limited to choice of interview format and questions. The interview result sets are analyzed separately, but it is the aim that their commonalities enable comparison between the various cases.

This common effort supports the reuse and comparison of the results in future work on the IRS model developed by Sveen et al[5]. At the time of writing, not all three studies are completed, and no such comparison has therefore been done yet.

4.1 Literature study

The results of this thesis are based on two parts: an extensive literature review, and a short field study. The literature study was performed to discover and summarize previous work done on the various subjects. This lays the ground for our discussions on the fit of incident reporting systems into information security, and the ability of the IRS model to describe such systems. It was therefore necessary to study

- how incident reporting is used in the field of safety
- how incident reporting is used in information security
- how researchers think incident reporting *should* be used, in both fields
- what challenges arise when we try to map safety thinking to information security.

Since our particular case is a health care institution, literature on incident reporting in health care was also studied. This was mostly patient / medical safety related (though today the distinction from information security is not so clear).

The literature study is by far the largest source of information for this project. As the literature study expanded beyond our initial estimates for time and volume, this reduced the time available for the field study (interviews) accordingly. The consequences of this are described in our discussion of the interview process.

Literature was found through different channels. The first set of sources we studied were those cited in the paper[5] on which we founded this project, and then sources extracted from these. In addition, we relied on the library database (BibSys) and scientific publications databases available through Gjøvik University College. These included IEEEXplore, SpringerLink, ScienceDirect, The ACM digital Library and Ovid. In addition, we searched the internet databases of the British Medical Journal, Journal of the Norwegian Medical Society and Lovdata[1] directly. The Google search engine was used as well, to aquire more information on various authors, such as possible connections to other

[1] Lovdata is an institution founded by the Norwegian Justice Department, for the purpose of creating and maintaining systems for legal information. Lovdata provides web access to all Norwegian laws and corresponding regulations.

authors, affiliations with institutions, clues to academic reputation, possible contact information etc. No sources to this paper were collected from Google alone, but we did find links to published articles that we had not found searching the research databases in which the articles were held (some of our search terms could have been better, in other words). On two occasions, there were exceptions to this last rule. A survey presentation was collected straight off the web, though only after researching information on the author (K. Aase) from the several of the official web-pages of the institution she was with, confirming that the presented research project existed and that the author was part of it. We feel confident that the information gathered was legitimate. The second web resource used directly was the history web site of IBM Corporation, where we gathered some details on the history of hard drive development. The information is somewhat insignificant and thus unlikely to be forged. The same information was also found on a number of other web sites, enough to convince us that it is an accepted truth that can be confirmed independently of said web page.

Generally we searched for terms like information, security, incident, event, reporting, handling, management, safety, model, modelling, System Dynamics, patient, medical, error, mishaps, near-miss, and an array of combinations thereof.

4.2 System dynamics modelling

The IRS model is based on System Dynamics, and although we perform no modelling in this project, understanding System Dynamics is essential to analyzing the model. In our discussion of the System Dynamics IRS model, we use causal loop diagrams to describe the links between various entities. These diagrams are mainly extracted from the original authors' model, using the Vensim modelling tool. For describing processes, flowcharts are a much used technique, and parts of the discussion could have been supported with these. However, since we are particularly interested in dynamic processes that employ feedback, we have kept to the notation of causal diagrams used in System Dynamics. Causal loops give very simple, easy to understand, descriptions of which entities affect others. Further descriptions of causal diagrams are given later, in the discussion on hypothesis extraction.

The project does not include creating a new model of our own, or performing simulation runs for testing of the existing model. This is outside what will fit into the scope and timeframe of the project. We base our discussions of simulation results on available literature.

4.3 Interviews

To find information on how well the model fits into existing ISIRS', we have chosen a purely qualitative analysis, through interviews with personnel at a health care institution. An alternative would be to design a set of quantitative metrics, or questions, that could be researched to find statistics on incident response times and rates, resolution rates, or particulars about how personnel experience the ISIRS (e.g. through graded questions, 1 to 5, agreed to not agreed etc).

However, for such questions, and statistics, to provide value, they must be very clearly defined, and respondents should be in significant numbers. For instance, for statistical analysis on a population of about 10.000, one could need a sample size of 1.000 (10 percent) to achieve necessary accuracy[6], and for smaller population, the sample proportion must be even larger. For qualitative studies (like interviews), such numbers are prohibiting. And it is argued that sample sizes for such studies need not be as large[7, ch. 3]. In fact, it can be argued that statistical averages over large samples only serve to diminish the value of findings[7, ch. 3]. Kvale does not go into detail about this, but we suspect that this is linked to how statistics tend to smooth out specifics. If it is the specifics you are after, then this is not a good thing.

To get a full quantitative picture of a very complex process, involving social issues, is a monumental task. It would among other things require that we quantify a range of qualitative measures, such as personnel motivation. We are, however, not looking to produce statistics or trend analyses, but rather to extract information on how the incident reporting system works for those affected. Another problem here would be that clearly defined questions are inherently exclusive. You will, at best, get the exact, "narrow" answer to your question, and risk to loose any additional information or explanations that relate to the answer.

We would rather give the respondent more freedom to express what he / she thinks is important, instead of confining him / her to our own interpretations. Thus, a qualitative research interview was considered the most fruitful method for our project. As Ragin[8] puts it:

> The key features common to all qualitative methods can be seen when they are contrasted with quantitative methods, Most quantitative data techniques are data condensers. They condense data in order to see the big picture.[..] Qualitative methods, by contrast, are best understood as data enhancers. When data are enhanced, it is possible to see key aspects of cases more clearly.

The qualitative research interview is most commonly associated with social or humanistic sciences, rather than technological disciplines. However, since we are indeed looking at human and social aspects of the ISIRS, we find it more appropriate to employ this method. We have tried to adhere to the definitions of the qualitative interview's main aspects as listed by Kvale[7]. The list is given in the appendices. If we have managed to take these properties into account in our interviews, we should be reasonably certain that the quality of the work is withing acceptable limits.

We do recognize, however, that interviews are a demanding form of gathering data, and it requires skill on the side of the interviewer to manage this partially structured approach. Simply asking the respondent to answer freely might not be enough, the interviewer must still be able to formulate his questions, and somewhat manage the dialogue during the intverview, so as to make it easier for the respondent to express what he really means. As novice interviewers, this could have an effect on what information we are able to gather.

To ensure validity and reliability of the results, we have followed guidelines from *(citation: "Practical Research")*. Note that since we are specifically gathering subjective opinions, authenticity of the results is considered more important than reproducability.

Accurately reproducing the results, from the same or other sources, might be impossible, since opinions vary with respondents and with time and context. Reliability in this context is then more concerned with internal consistency, ie. whether the data gathered are plausible, given what we know about the people or events involved[6, chapter 13]. In reviewing the answers we got, we have not come across any reason to suspect that respondents did not answer truthfully.

4.3.1 Interview questions and respondents

We formulated a set of open questions, relating to the ten hypotheses we believed to be the most central to verifying the model's assumptions[2].

The interview questions were adapted to three different types of respondent. For regular staff, we asked how they perceive incident reporting and the organizations commitment to it. For security personnel, we asked the same, but also more about the actual workings of the system. For the last group, managers / policy makers, we also asked how they percieve the ISIRS, and we tried to establish what management is doing to show commitment to incident reporting, and ensure successful use of it.

The number of respondents necessary for the interviews to provide value can vary greatly with the subject. A common number for qualitative interviews is said to be 15 +/- 10[7, chapter 3]. We initially planned to interview nine people, and regarded six as a minimum, since we would need more than one respondent of each type to protect respondents' anonymity within each group. However, we did not reach our goal of nine within the available time frame. Instead, we only interviewed three people. This forced us to make some changes to the format of the interview.

First, we ended up *not* dividing respondents into three groups. At the same time, we removed the interview questions that were specific to security personnel and managers. Unfortunately, this meant we did not get all the info we wanted, but we still covered most of the original points in the interviews. The biggest loss with this change is perhaps that we were unable to compare replies across functions. For instance we cannot measure whether similar issues are viewed differently by staff and management. We can, however, still compare how various staff see incident reporting, in comparison to the organization's established policies.

The initial interview protocol (or set of questions) was modified as a result of feedback from the first respondent.

Details on the interview questions and respondents are given in chapter 7.

4.4 Ethics

Multiple ethical considerations must be taken both in planning and execution of any research. Considerations vary with the type of research, and of course, the type of information one deals with. For the literature study, we have sought to use information sources

[2] There were many more hypotheses extracted from the model, but to keep within a realistic scope for a masters project, we limited our choice to ten

that are verifiable, ie. cited by (multiple) known authors, or that are known to have been subjected to thorough scrutiny. At the least we consider whether the information given appears plausible, and can be found in other sources as well.

5 Review of previous work

Here follows a summary of information sources and current literature, we used as a basis for the thesis project. Our literature list is by no means exhaustive for the respective fields, but we hope we have covered a representative set.

Sources reviewed include ones that pertain to System Dynamics, information security, incident reporting and safety science. Sources specific to the health care sector are also included.

5.1 System Dynamics modelling

The basis for the thesis assignment is [5], a paper that initially adresses "secure knowledge management" in general. The paper lists some of the influences on secure knowledge management programs. It also presents a causal model and simulation study of how information sharing is influenced (by many factors). The presented model is the generic example that forms the basis for this thesis project.

The incident reporting system is seen as a form of secure knowledge management system, bearing similarities in purpose and what influences they are under. The term "incident reporting system" is perhaps too narrow, since the modeled system also considers how the organisation learns from incidents, and the effects this learning has on incident occurence.

Key points here include: The authors describe what they term a duality in secure knowledge management: (1) the securing of knowledge and (2) the management of security knowledge. (1) is traditionally the motivation behind security efforts, but as is pointed out, (2) is important in learning from past experiences and building security consciousness in an organisation. Incidentally, an information security incident reporting system would fill a role in both (1) and (2), as it would not only help manage information about security incidents, but also contain (and need to secure) an amount of sensitive information itself.

Through simulations (based on the model), [5] shows how an incident reporting system could strongly affect incident occurence under the right conditions. Sveen and others have also created a newer version of the model, targeted at information security[9]. This work was published after we started our own work, and we refer to, but have not based this project on that version of the model.

With origins at least back to the late 1950's[10], System Dynamics is a methodology for studying complex systems as a collection of feedback relationships. By modelling the structure of a system, and how critical parts of it reciprocally affect each other over time, one can identify systemic causes to (emergent) problems, and accordingly suggest improvement to the structure of the system[11]. By focusing on a system's structure rather than every part and detail, one hopes to be able to grasp problems at their (systemic) root, rather than at a more superficial, or symptomatic level. System dynamics has developed into a powerful analysis tool, and the field is still evolving. Over time, various generic structures (i.e. templates) have been built, that identify common architectural concepts. For the kind of model we discuss in this thesis, we limit ourselves to the type termed "system archetypes". From their origin around 1990 [12][1] system archetypes have been developed by many, both for general system dynamic modelling, as well as specific fields. We have looked to [13, 14, 15] for a lot of our background information.

A notable contribution was made by Wolstenholme [13, 15], who showed that all of these archetypes could be described in terms of four generic archetypes. These archetypes each described a common problem, and Wolstenholme created a corresponding solution for each of them. Look to chapter 6 for a description of causal loops, and an example of a basic problem archetype.

Having these generic structures to look to makes it easier to extract insights from models, and to identify solutions to problems. If you can look at a complex model, and identify it as corresponding to a known archetype, you immediately know something about how that model behaves, and why. This helps to show how your model might be simplified, or perhaps how a particular problem can be solved, since for each archetypal problem, Wolstenholme already presented a solution.

The two cited works by Wolstenholme also points to the importance of recognizing how organisational boundaries affect behaviour of an organisation (or system). Eloquently put, "*they exist - and cannot be ignored*" [13, p. 343].

In [14], Marais and Leveson propose how system archetypes can be use to model organisations in accident analysis, including a discussion on incident reporting. The paper provides good examples on how systems fail through unintended consequences of poor safety design, and on how fixing symptoms only serves to hide root causes.

Rich and Gonzalez [16], Gonzalez et al. [17] and Gonzales[18, 19] demonstrate how System Dynamics models can serve as aids in improving safety or information security. Of particular intererest is the lesson that

> "Though little hard data was available, the participants' knowledge of [..] their environment was sufficient for credible [..] causal modeling", [17].

In other words, they didn't need accurate measurements and analyses, it came down to participants' (qualitative) understanding.

5.2 Incident reporting and safety science

Incident reporting (IR) is core to traditional safety science. However, according to a recent study by Nielsen et. al [20], empirical evidence of the effectiveness of IR is hard to come by. Most sources found through the work in that study were unscientific or anecdotal, not useful for drawing scientific conclusions. Nielsen et al. studied the implementation of IR systems at two metal production plants in Denmark. The study was not conclusive on whether IR is actually effective, but did suggest an inverse releationship between the number of reported events (smaller incidents and near misses) and the number of serious incidents occured, in accordance with the findings in [21]. Kjellén[22] also cites several sources that support this. These findings are also in accordance with a very old, and apparently debated, theory that (according to Nielsen et al.) has yet to be proven. They refer to the work of H. W. Heinrich, dating back to 1931. The sources

[1] Generic structures have been developed by many, but Senge seems to be the one usually referred to when the origin of the "system archetype" concept is mentioned.

we have examined cite several editions of Heinrichs work. The latest we know of is from 1959[23]. Heinrich is by many considerd the "founding father" of safety science. His hypothesis was that "minor" and "major" incidents have the same underlying causes (Johnson [24] also builds on this idea).

Underreporting of incidents and events is naturally the first big obstacle that must be tackled in IR. An incident reporting system without incidents, or a statistic with flawed data is useless. The general idea is to encourage the reporting of all incidents, no matter how mundane or insignificant they may seem. At the same time one must make sure that the person who files the report is not punished for doing so, even if reporting has drawn negative attention to the person or organization[2] ([5, 20, 24, 25, 26, 27] are sample proponents of this view).

Underreporting is also cited as a major factor in [28], which presents arguments for analyzing incident reports to identify accident precursors. Fear of repercussions are highlighted as a major contributor to underreporting.

In Cooke[29] and Cooke and Rohleder[27] one suggests discarding the view that disasters (like any incidents) are inevitable in complex systems, replacing it with the view that a "high-reliability" organization has properties or mechanisms that make disasters preventable. This is not to say that all incidents are preventable. On the contrary, they focus on learning from (minor) precursor events that will inevitably occur, at least occasionally, in order to avoid major events (disasters). The path to high-reliability safety performance, they say, goes through "incident learning systems", ie. the organisation-wide, systematic collection and extraction of information (lessons) from incidents, as opposed to the limited, "local" learning achieved from each singular incident. This would enable an organisation to, for example, recognize the occurence of (more or less) the same incident in different locations, or at different times. The authors present a model for an incident learning system, based on viewing incidents as an output of the business[29], much the same way as any regular product, and subsequently handling them in a "continuous improvement cycle", principally in the same way one would handle a regular product quality issue. An important point in the process is "incident recall": to not just implement corrective actions specific to an incident, but analyzing past incidents to discover failure modes yet unknown, thus performing proactive incident management.

Johnson [24] has written an impressive and and enlightening book on using incident reporting for managing safety. Only a few chapters were reviewed in any depth, the book's size precluded a complete review in the available time[3]. Johnson points out that

> "The higher frequency of less critical mishaps and near-miss events also supports statistical analysis that cannot reliably be performed on relatively infrequent accidents", [24, p. 21]

Johnson present a series of arguments for doing incident reporting, and of the more interesting is that incident reporting not only helps discover what fails, but can also help discover what works (ie. why did this incident not esacalate to something worse?). This provides valuable feedback on existing safety or security mechanisms. Johnson also

[2] Punishing willful, malicious action leading to the incident is, of course, another matter.

[3] We restricted ourselves to chapters 1, 2, 4 and 5, parts of chapters 6, 8 and 10, and chapters 13 and 16

argues that IR is cheaper than accidents [24, p. 22]. Throughout his book, Johnson also presents a thorough discussion, with examples, on the pitfalls that threaten effective incident reporting systems, particularly dealing with how to encourage contributions to the IR system. These problems include anonymity, legal issues, and placing of blame ("proportionate blame"). An interesting example given is how some workers (pilots), counterintuitively are more likely to report incidents, despite the fact that they might have a lot to loose (pp. 36-38).

Another seminal work, published recently, is that of Wallace and Ross [30], who practically pick todays safety science practices to pieces, and argue for a change in which psychological, philosophical and scientific methods and theories are employed in safety science. Specifically they criticise how reporting systems and investigation efforts are mainly launched from the wrong starting point[30, p. 60]. There is also a chapter on Systems Theory and how viewing systems as dynamic feedback mechanisms (which is what System Dynamics does) could be a path to follow. They also discuss how our perception of error is somewhat skewed[30, ch. 5]. We tend to treat error as something unconditionally bad, however trial and error is an integral part of learning. Ironically, without errors, we cannot learn to prevent them. Others, for instance Marais and Leveson [14], make practically the same point, showing that an error-free environment itself could create a higher risk for error.

Sonnemanns et al[31] paints a disturbing picture from the Ducth chemical industry, where they argue that all of the accidents they analyzed could have been predicted. The failure to do so was, in part, that organizations did not take into account the effects of, for instance, organizational changes. Accordingly, the right factors and information were not analyzed in their efforts to reduce accidents, even though the necessary precursor information was on the table. Sonnemans et al. also promotes the view that that events can/will lead to incidents, similarly to [5, 28].

Another somewhat worrisome result was produced in a transportation safety study by Chapman and Underwood[32]. Drivers asked to recall all near-accidents (and accidents) they were involved in, over the past 14 days, only remembered an estimated 20% of the events. This was in comparison to a group that was asked to record every event, on tape, immediately after it took place. This even happened for quite serious events.

5.3 Incident reporting and information security

As we move to information security, we see how other authors have previously drawn on safety research as a basis for developing information security practices. We have already mentioned Sveen et al[5]. Related to this is the System Dynamics work by Gonzales et al[17] and Gonzales[18, 19].

There is, however, not too much literature to be found on employing a whole incident reporting process, like the one we discuss in this project. There is a lot of standardization, regulation, audit and information assurance requirements etc, for example [33, 34, 35, 36, 37, 38, 39], but these mostly present general demands ("some control process must exist"), or they deal only with specific ares / measures for information security. For instance, the Personal Data Regulations[38] demands that all accesses to personal data be logged, that *security measures shall prevent unauthorized use of [..] information*, and that *attempts to make unauthorized use of the information system shall be registered*[37, Section 2.14], but says little of the process surrounding this.

Work on building an actual process is scarce (which is what spawned this project in the first place).

In [40], Stoneburner discusses unifying risk taxonomies from both safety and security, to improve the coupling of the two related fields. The article shows good example of how the differences between the two fields can be merged.

But even if we can reuse concepts and thinking from safety science, that only aids us so far. Information security, insofar as it these days to an extent equals computer security, will still be faced with challenges that that threaten to void IR usefulness. For instance, incident reporting will typically be handled and followed up by a computer security incident response team (CSIRT) of some type [41]. Wiik et al[42] describe how an overworked CSIRT, trapped in "firefighting mode", will likely not be able to extract lessons or necessary output from incidents to be fed back into the organization for learning and prevention. With incident and vulnerability reports on the rise [18], the danger of this happening is increasing.

5.4 Incident reporting in the health care sector

Looking to the health care sector, we find that analyzing incidents (which necessitates reporting) is common practice, and advocated by many. It is also a field riddled with challenges. A student paper from Bergen University in Norway [43], explores medical treatment errors and reporting culture at a particular hospital, and discusses the need for good reporting culture to learn from and avoid future errors. The paper projects that in Norway as many as 1600 deaths every year are caused by medical errors.

Vincent[44] and Sari et al[45] argue that reporting systems are generally not adequate, and also points to problems of severe underreporting. Both papers argue that retrospective case reviews are much more effective for discovering errors, than what incident reporting systems are.

[46] supports the view that little is to be gained from vast incident reporting, and suggests that since we already know there is a problem, further incident reporting is unecessary, and efforts should be concentrated on improving quality instead.

A norwegian health issues tv-show[47](NOTE: Better reference to be added) discussed the frequency of medical errors in norwegian health care institutions, and presented arguments that most errors had systemic causes. Still, staff were unwilling to report them, out of fear of repercussions.

Fears of repercussions and shaming are quoted as key factors for underreporting also by [28]. Person-oriented "blame culture" is frequently listed as a problem, like in [48, 49]. Some also point to the lack of feedback as demotivating for reporting, for instance [50].

A recent survey by Kommunalansattes Fellesorganisasjon, a Norwegian union for public services employees, reveals that 86 percent of health care professionals say it is common to access patient records beyond what is necessary for patients' treatment [51]. Recent audits of electronic patient journal systems at three Norwegian hospitals, have also revealed that access control and audit mechanism in these systems are lacking, and sometimes not at all present[52, 53, 54]. One of the hospitals was in 2005, after a previous audit, required to correct several problems with access to patient information. The recent audit revealed that some of these issues were resolved, some were resolved but quickly introduced again, and other were never adressed[52][4].

In addition to the various systems used in day-to-day patient care, there is also a large number of general and speciality health registers that hold data about many different aspects of people's health[55]. It is no bold assumption that most or all of these exist in some electronic form today. One issue here is the use of the unique personal identification number, which is widespread in such registers. Information spread throughout many different registers can potentially be linked to the same person, even though each source might only hold a few details.

On a positive note, efforts are under way in Norway for bettering the standards of health information systems, for instance through KITH[5], a government owned company that performs IT-standardisation, and IT-contracting, for the health and social services sector(e.g. [56]). Legislation and central regulations have also increased in their requirements on information security, in line with the increas in use of IT, for the health care sector[35, 57, 38, 37, 58]

In a health care case study, Amoore and Ingram[59] suggest a *feedback note*, highlighting positive actions taken by the people involved, as a tool for learning from incidents. This was apparently an effective way of increasing organizational learning as a result of incident reporting and investigation. The article refers to a study on incidents involving medical equipment, in an environment where the tradition evidently was to end investigations after discovering only the immediate causes of the incidents. The feedback note contained information on the incident, what happened, what kind of device was involved, which possible causes were found, but most importantly, which actions by staff helped minimize effects of the incident. By focusing on positive actions, it helped put a positive ring to the feedback that went to the staff, making it easier to give such feedback, and correspondingly inviting investigating staff to look past these causes, and highlight good practices that were used, or could be implemented, to reduce risk of adverse events.

[4] Some issues were not adressed pending replacement of the journalling system itself. That a system of such poor quality could have been implemented and used at all, is perhaps an argument in itself for a stronger effort in incident reporting.

[5] Kompetansesenter for IT i Helse- og Sosialsektoren, http://www.kith.no/

6 The IRS Model

We now turn to the System Dynamics model of Sveen et al[5], and the hypotheses that were extracted from breaking the model down into its basic parts. We first give an introduction to causal loop diagrams, which is what the model diagram is made up of.

6.1 Causal loop diagrams

The model is shown using causal loop diagrams, a simple construct showing how various entities affect each other. Causal relationsships are described in terms of variables *positively* or *negatively* affecting others. Variable X *positively* affects Variable Y when an increase in X leads to an increase in Y, and a decrease in X leads to a decrease in Y. Variable X *negatively* affects Variable Y when an increase in X leads to a decrease in Y, and correspondingly, a decrease in X leads to an increase in Y.

In it's simplest form, a causal loop diagram (figure 1) has two entities which both affect each other (otherwise it would not be a loop)

We borrow basic examples from Wolstenholme[15] to show how these loops work. A simple causal loop is shown in figure 1:

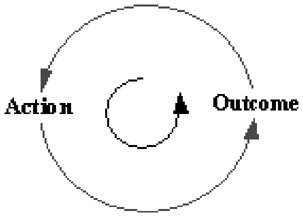

Figure 1: Basic causal diagram

However, for any (intended) action, there could be one or more unintended reactions in the system or organisation. This can be shown by adding the reaction to the diagram, and linking it with the outcome, as in figure 2. Such unintended consequences are often hidden behind organisational boundaries, which is why these are so important to identify[15].

In figure 2, the loop marked I shows the *intended outcome* loop, while U marks the *unintended result* loop. This kind of combination of two loops forms the basic building block of Wolstenholme's system archetypes.

Figure 3 shows a specific situation that can be modelled like this.

When the effort in "Sales" increase, so do the number of "Orders". The increased volume, creates more income to boost sales efforts (and so does the reputation of a successful product). The two variables, "Sales" and "Orders" positively affect each other, denoted by the plus-signs next to the arrowheads on the links[11]. The plus signs show what is called the *polarity* of the links. Since this is an "ever-increasing" loop, we term

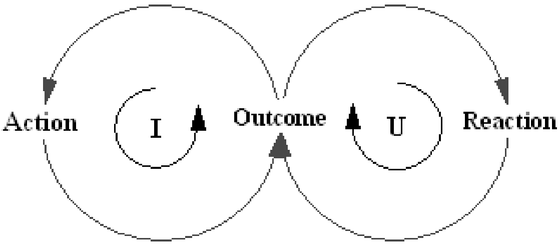

Figure 2: Basic causal diagram 2

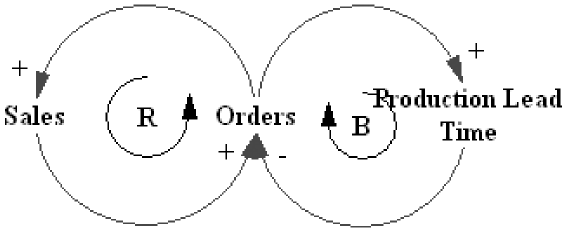

Figure 3: Sales Problem

it a *reinforcing* feedback loop, denoted by the R and the directional loop drawn in the middle.

However, with the steady increase in orders, eventually production capacity is overloaded, and the time before ordered items can be produced starts to increase. This, in turn, limits (*negatively* affects) the number of orders effectuated, as shown in the right half of figure 3.

What happens here is that the negative impact (note the minus-sign on the arrow) of "Lead Time" on "Orders" is balanced against the increase that "Orders" causes in "Lead Time". This second half of the causal diagram therefore constitutes a *balancing* feedback loop, denoted by the B. In sum, this balancing loop holds back, or cancels, the increase caused by "Sales". The sales department somehow didn't see how their effort (for instance a sales campaign) had an effect on manufacturing, and that this would impact sales again. Somehow, there is an organisational boundary between the two departments.

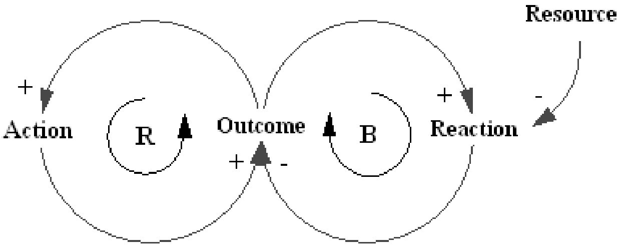

Figure 4: Underachievement problem archetype

This particular situation is known as an *underachievement archetype* (figure 4). The expected performance of the reinforcing loop is not seen, because the unintended, balancing loop holds it back. The solution to this problem lies in using some of the intended effort to counter the unintended reaction. Typically, the reaction is caused by a resource constraint somewhere in the system (which we added to figure 4), and so the solution is to unblock this constraint (figure 5).

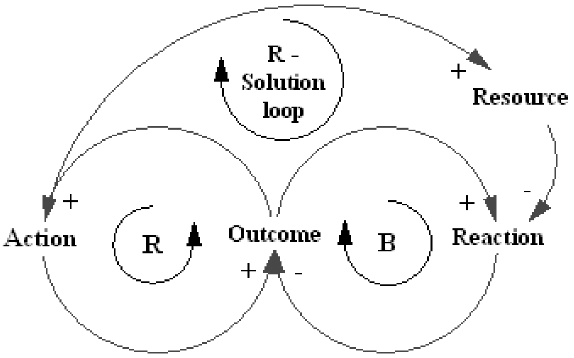

Figure 5: Underachievement solution archetype

For our sales example, the specific solution could be to use some of the sales effort, eg. a sales forecast, to adjust manufacturing capabilities to keep up with the sales volume[15, p. 15] (figure 6).

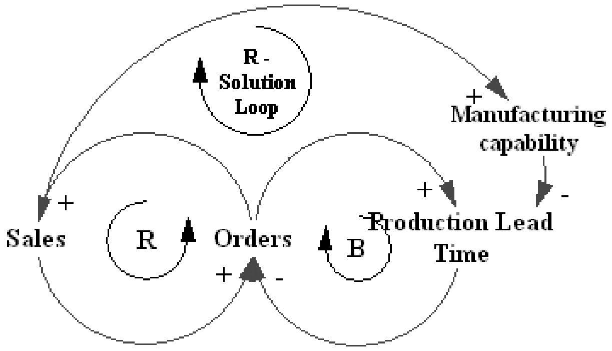

Figure 6: Sales Problem Solution

These were some general ideas of causal loops and archetypes. When using such models for simulation, different weights and calculations are assigned to each of the entities/variables in the diagram, and therefore the power of each loop can vary, and the balancing loop might not be high enough to restrain the reinforcing loop. The finer points of this is not an issue for us at the moment, as we are not performing simulations.

The final piece of knowledge we need before continuing is that, as can be seen in the preceding diagrams, when we have an odd number of negative (-) polarities in a loop, we get a balancing loop. Accordingly, with an even number of negative polarities we get a reinforcing loop (one could say that with every two minuses their overall negative effect "cancels out").

6.2 Background on the IRS model

The concept behind the ISIRS is thoroughly described in [5], and we wil try not to repeat too much of it here. Instead we give a brief description of the model and it's purpose, and then move on to splitting up the model into its various parts.

As mentioned before, [5] initially adresses "secure knowledge management" in general. The paper lists some of the influences on secure knowledge management programs. "Secure knowledge management", here referring both to secure management of knowledge/information, and to management of security knowledge. That is, we are talking about secure information (a general goal for the organisation) and security information (i.e. the information that the ISIRS processes).

Securing information is generally regarded as very important, but in all environments resources are limited, and it is hard to predict just how much it is worth to spend on securing information. Furthermore, information sharing, as incident reporting really is, can be difficult to achieve in many organisations. This can be for competitive reasons, or from fear of loosing face because of a disclosure. It could also be because of a lack in resources, or a lacking awareness of the importance of collecting security knowledge to battle security problems. [5, 20, 22, 24, 25, 26, 27] all discuss reasons for why organisations experience reluctance to reporting.

The IRS model was based on cases from several industries, and was built to identify in what way many of the mentioned problem factors influence each other, in order to find how the problems can be overcome. An effective, well working, reporting system is after all key if organisations are to consider it worth the investment. The authors suspected that there was a common structure to incident reporting in all the cases, since they all seemed to exhibit the same problem behaviour. This would make System Dynamics modelling ideal for tackling the problems.

Having created a model, simulation runs with varying parameters were done to simulate the incident reporting system's behaviour under different conditions. Sveen et al[5] showed that under the right conditions, incident reporting could significantly improve (ie. reduce) incident occurence. They found vast differences in behaviour depending on condidtions, with recriminations against reporters, and lack of resources to follow up on reports, seemingly being the most detrimental factors.

We will now look closer at the model itself, and return to the model's behaviour in the discussion on whether it is fit for information security incident reporting.

6.3 Details of the IRS model

The starting point of the model is that there is a certain amount of events and incidents occuring in the organisation. In the diagram (figure 7) it is represented by the "Base Event Occurence Rate", and the "Event Occurence Rate". The model does not concern itself with how or where events and incidents come into being. Therefore the only re-

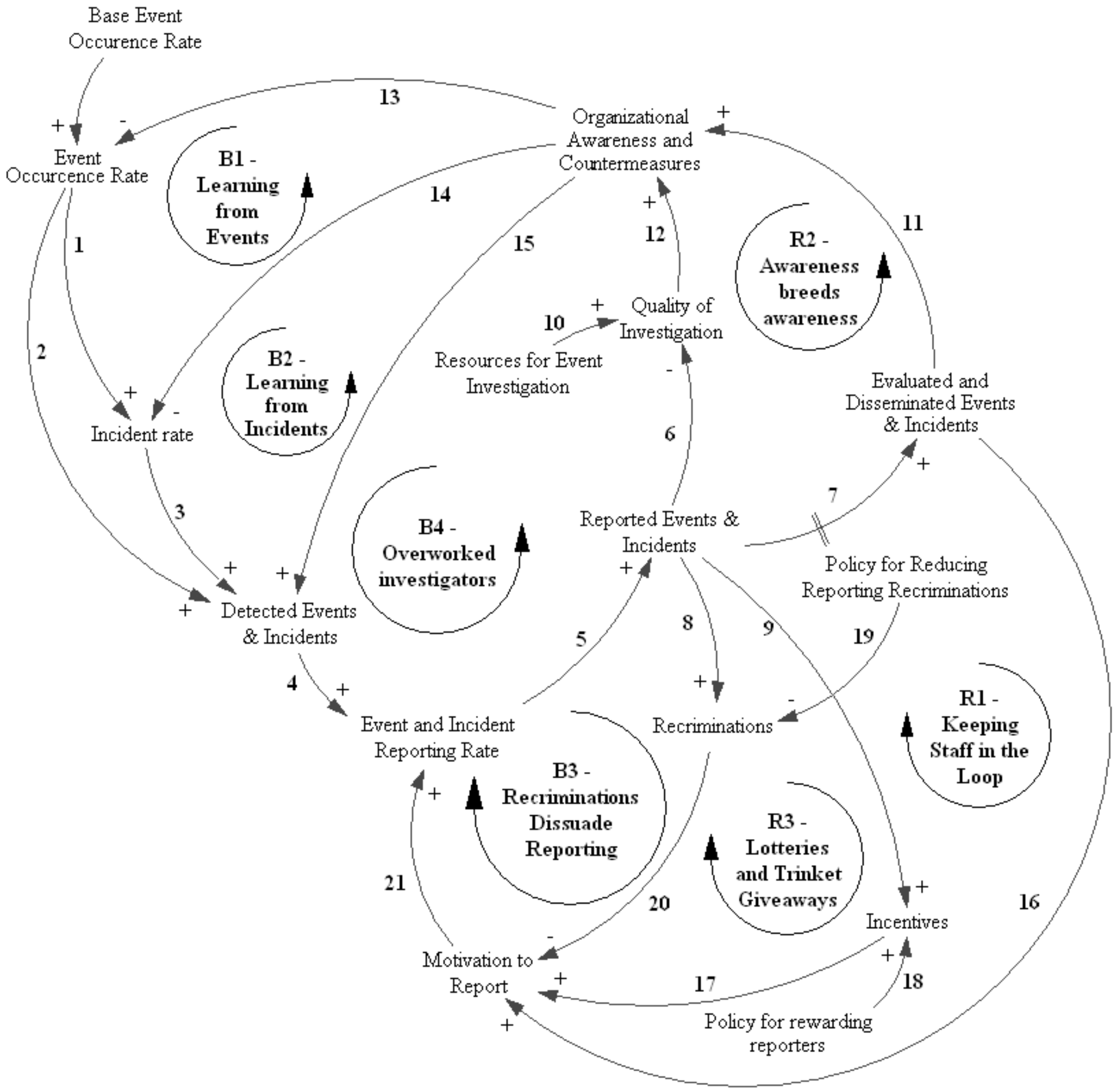

Figure 7: The IRS model

leationship modelled in this respect is "Base Event Occurence Rate" and the potential for incidents created by occurence of events. Of all events taking place, some eventually become incidents if they are not mitigated (it is assumed). Event and incident occurences lead to a certain number of events and incidents being detected and reported. From there on, all the various aspects of the model spread out.

6.4 Links

We start by looking at each link in the model, considering a statement about the model's behaviour. Many are trivial, some deserve a more thorough discussion. The numbers in figure 7 refer to each statement below. Note that most of the descriptions apply to events and incidents alike, but for simplicity we only use the term events here, unless where there are explicit differences. Also, the terms "evaluate" and "investigate" are used interchangeably. Both expressions were used in the IRS model creators' paper.

Variable	Affects	Variable
Event Occurence Rate	positively affects	Incident Rate
Event Occurence Rate	positively affects	Detected Events & Incidents
Incident Rate	positively affects	Detected Events & Incidents
Detected Events & Incidents	positively affects	Event & Incident Reporting Rate
Event & Incident Reporting Rate	positively affects	Reported Events & Incidents
Reported Events & Incidents	negatively affects	Quality of Investigation
Reported Events & Incidents	positively affects	Evaluated Events/Incidents
Reported Events & Incidents	positively affects	Recriminations
Reported Events & Incidents	positively affects	Incentives
Resources for Event Investigation	positively affects	Quality of Investigation
Evaluated Events/Incidents	positively affects	Awareness
Quality of Investigation	positively affects	Awareness
Awareness	negatively affects	Event Occurence Rate
Awareness	negatively affects	Incident Occurence Rate
Awareness	positively affects	Detected Events & Incidents
Evaluated Events/Incidents	positively affects	Motivation to Report
Incentives	positively affects	Motivation to Report
Policy for rewarding reporters	positively affects	Incentives
Recriminations	negatively affects	Motivation to Report
Policy for reducing Recriminations	negatively affects	Recriminations
Motivation to Report	positively affects	Event & Incident Reporting Rate

Table 1: Textual representation of model's causal links

Statement 1 *Event Occurence Rate positively affects Incident Rate*

Increase in number events (i.e. near-misses) leads to increase in number of incidents. This is based on the assumption that events and incidents have the same underlying causes, or even that an event can be a direct precursor to an incident. Correlations between the numbers of events and incidents have been shown in safety research, though some evidence to the contrary have also been published(see for instance [24, ch. 2]). It is not given that this will be true for information security. For instance, Johnson points to evidence that this causal relationship exists for some types of events more than others.

Statement 2 *Event Occurence Rate positively affects Detected Events & Incidents* and

Statement 3 *Incident Rate positively affects Detected Events & Incidents*

As the number of occuring events rise, so does the number of detected events. This only presupposes that the probability of detection is non-zero, or that the organisation is at all capable of detection. It should be safe to make this assumption, and we will not elaborate on this.

Statement 4 *Detected Events & Incidents positively affects Event & Incident Report Rate*

As events are detected, someone will report some of them, thus influencing the reporting rate. According to the model's creator, the rate is defined as reports per time[1]. That is, more events detected in a given amount of time will increase the rate. The rate of detected incidents that are actually reported is not considered here.

Statement 5 *Event & Incident Reporting Rate positively affects Reported Events & Incidents*

The assumption is that as more of the detected events are reported, the number of reports increases. This is a rather safe assumption.

Statement 6 *Reported Events & Incidents negatively affects Quality of Investigation*

Unless resources available for handling reports are infinite, then as the number or reports increases, there will inevitably be less handling resources available per report. Ultimately, the resources could be exhausted, or at least "outpaced", so that reports will come in faster than they can be handled. Either way, this lowers the quality of the report handling. This effect is supported by both common sense, and for instance literature on CSIRT performance[42].

Statement 7 *Reported Events & Incidents positively affects Evaluated Events/Incidents*

As more events are reported, more will be handled, thus increasing the number of evaluated events. The true effect of this is, of course, dependent on that there are resources available to do the handling/investigation.

The double line on this particular arrow denotes a time delay, indicating that there is a (notable) passage of time before the change in one factor affects the other. In this particular case, it shows that from a report is filed, there is a delay before the investigation result is available. One can imagine many other possible, variable delays between model factors, but to avoid complicating the drawing, these are not inserted. We assume this one was left since it is noticeably present in all cases.

Statement 8 *Reported Events & Incidents positively affects Recriminations*

[1] personal communication with F.O.Sveen

Given that reporting of adverse events is punished, then an increase in number of reported events would also give an increase in number of recriminations against reporters.

Statement 9 *Reported Events & Incidents positively affects Incentives*

Similar to statement 8, if we assume that there is a culture for rewarding those who report events, then the number of rewards would increase with the number of reports.

Statement 10 *Resources for Event Investigation positively affects Quality of Investigation*

Corresponding to statement 6, if we add more resources for investigation, this should increase the quality of investigation. (Assuming that these resources are put to good use)

Statement 11 *Evaluated Events/Incidents positively affects Awareness*

Each evaluated event or report adds to the total knowledge of the organisation. The increased knowledge should lead to heightened awareness, but this is under an assumption that the knowledge is somehow spread to those who can subsequently detect events. I.e. the knowledge must not be "filed and forgotten" by the event handlers, but rather fed back into some organisational learning system.

Statement 12 *Quality of Investigation positively affects Awareness*

Higher quality investigations will provide more and/or better insight into the causes of events. This should improve the quality of the information incorporated into the organisational learning. If personell is equipped with more accurate information on events and their causes, they should be better prepared to spot them.

Statement 13 *Awareness negatively affects Event Occurence Rate*

and

Statement 14 *Awareness negatively affects Incident Occurence Rate*

As awareness increases, the number of events caused by mistakes and errors should decrease. Heightened awareness should also lead to higher quality in preparations of regulations, procedures, specifications etc, thus helping to remove old flaws that could cause future events. We dare speculate that for these events, if this effect is not seen, it would be a sign that there are deeply rooted systemic causes to the events, rather than human errors.

At the same time, since many events in information security are deliberate attacks, the effect of awareness could be inherently limited. We can imagine, however, that the effect would be greatest on events caused by insiders (who would know their co-workers are more aware), than on events of external origin (ie. hacker attacks via the Internet). It seems then, that awareness would have a different effect depending on where an event originates.

Statement 15 *Awareness positively affects Detected Events & Incidents*

Heightened awareness would, naturally, make personell better detectors of adverse situations.

Statement 16 *Evaluated Events/Incidents positively affects Motivation to Report*

A significant motivational factor for reporting is that reporters see the usefulness of their effort. They must therefore be "kept in the loop"[24], and receive feedback on how the event is handled, and the lessons learned from it. This comes in addition to the feedback to the organisation in general (statement 11).

Statement 17 *Incentives positively affects Motivation to Report*

If people are rewarded for reporting, this should increase their willingness to report. Note though, that incentives could introduce bias in the reporting. It could, for instance, lead to reporting of issues that are of no relevance or interest, merely because the reporter wants to cash in a reward. This could affect both the organisations event statistics, and consume resources better spent on handling more important events.

Statement 18 *Policy for rewarding reporters positively affects Incentives*

and

Statement 19 *Policy for reducing Recriminations negatively affects Recriminations*

These should need no elaboration.

Statement 20 *Recriminations negatively affects Motivation to Report*

People are not likely to do anything they will be punished for. Recriminations can therefore quickly cancel the effects of personell's willingness to report, whether this comes from rewards or just their sense of duty (or morals, for that matter). As with rewards, recriminations can lead to reporting bias. It is inherent in the idea of recriminations that reporters 1. Can get punished for the error they might have made that led to the event, or 2. Can get punished for "blowing the whistle" on something the organisation (or co-workers) would rather not bring to light. In either case, one can expect that the more serious the event, the stronger the repercussions. This could lead to underreporting of serious events. The most dangerous of recriminations are those that are not official, policy mandated actions, but hidden punishments from colleagues or managers who might, for instance, hold a grudge against what is felt to be a disloyal member of the organisation.

Statement 21 *Motivation to Report positively affects Event & Incident Reporting Rate*

As personell are more motivated to report, one should see an increase in reported events. This builds on the assumption that there is underreporting in the organisation, ie. that some detected events go unreported.

6.5 Loops

We now turn to the causal loops of the model, which are the main structures that make up the model. The loops are combinations of elements/variables from the model. Each loop in itself represents a hypothesis or statement about the system's behaviour. The loops have been drawn in separate diagrams, and have been reshaped a little, to save some space. They are thus shaped slightly different than if you lifted them straight out of the original model, however the link numbers remain the same.

Loop	Description
B1	Learning from Events
B2	Learning from Incidents
B3	Recriminations dissuade reporting
B4	Overworked Investigators
R1	Keeping staff in the loop
R2	Awareness breeds Awareness
R3	Lotteries and trinket giveaways

Table 2: Textual description of model's causal loops

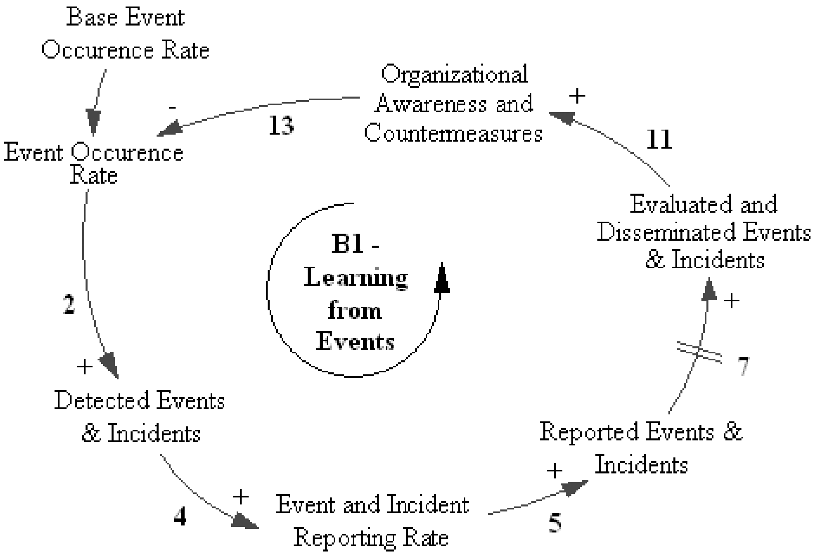
Base Event
Occurence Rate
Event Occurence Rate
Organizational Awareness and Countermeasures
-
13
+
11
Evaluated and Disseminated Events & Incidents
B1 - Learning from Events
2
+
Detected Events & Incidents
+
7
Reported Events & Incidents
+
4
+
Event and Incident Reporting Rate
5

Figure 8: Loop B1: Learning from Events

Statement 22 *Learning from events reduces future events (and incidents)*

(Loop B1, figure 8) As events occur, at a certain pace (Event Occurrence Rate), a certain number of them will be detected and reported. As the number of reports increase, so (over time) does the number of investigated events. The knowledge gained increases awareness in the organisation, which in turn reduces event occurrence, thereby creating a balancing loop. In the IRS model, fewer events also lead to fewer incidents. For simplicity, this link between loop B1 and B2 is not shown here. See Loop B2.

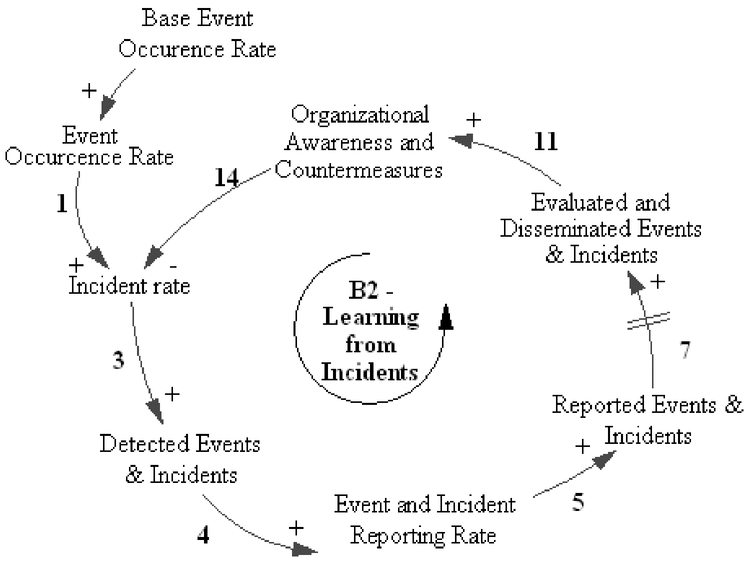

Figure 9: Loop B2: Learning from Incidents

Statement 23 *Learning from incidents reduces future incidents.*

(Loop B2, figure 9) As incidents occur, at a certain pace (Incident Occurrence Rate), a certain number of them will be detected and reported. As the number of reports increase, so (over time) does the number of investigated incidents. The knowledge gained increases awareness in the organisation, which in turn reduces incident occurrence, thereby creating a balancing loop. This loop is also affected by the Event Occurence Rate (Statement 1).

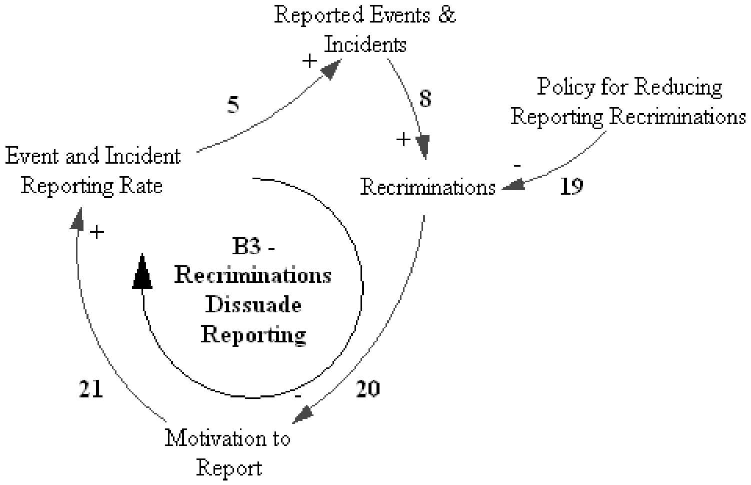

Figure 10: Loop B3: Recriminations Dissuade Reporting

Statement 24 *Recriminations dissuade reporting*

(Loop B3, figure 10) As a report is filed, the reporter is punished. This makes the reporter less likely to report in the future, thus lowering the reporting rate. This would likely have a deterring effect on other reporters, as well. See Statement 20. The loop can be affected by measures to reduce recriminations. itself.

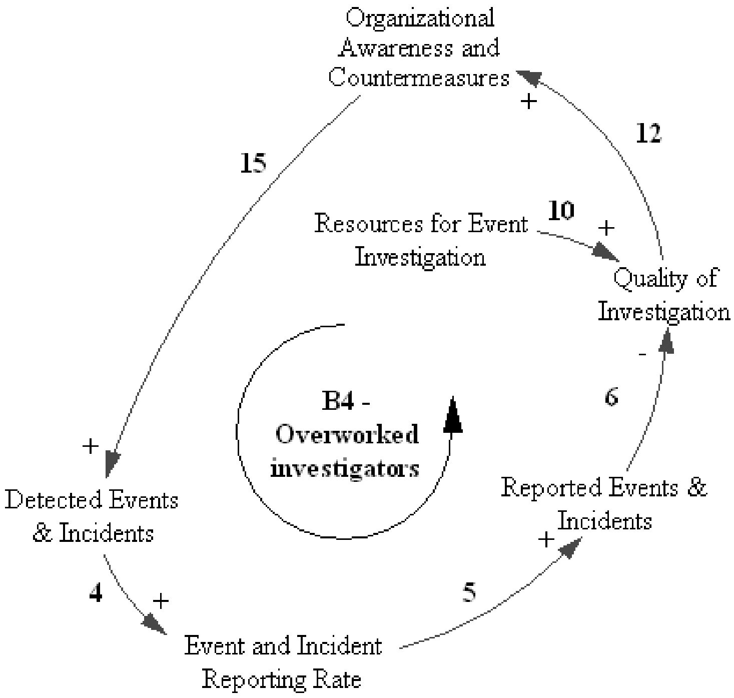
Organizational Awareness and Countermeasures
+
12
15
Resources for Event Investigation
10
+
Quality of Investigation
-
6
B4 - Overworked investigators
+
Detected Events & Incidents
Reported Events & Incidents
+
4
+
5
Event and Incident Reporting Rate

Figure 11: Loop B4: Overworked Investigators

Statement 25 *Insufficient investigation resources reduces reporting*

(Loop B4, figure 11) This balanced loop creates a real effect on the reporting system, but maybe not the effect that is intended or expected in the model design. Let's trace the loop: Available resources directly affects the Quality of Investigation. Quality positively affects Awareness[2], which has an effect on the number of Detected Events & Incidents. As the number of subsequent reports increase, investigation resources are exhausted. This balances the loop, since when quality deteriorates, so does Awareness, and with it the detection capability. However, the effect of inadequate resources described with the presentation of the model in [5], is not quite the same. This turns out to be because of a difference between the simulation model and the causal model[3]. Here is how [5] describe the scenario where "Limited resources" is simulated:

> "Scenario 'Limited Resources' has fewer resources assigned to investigation than what is actually needed to investigate, causing an accumulation of unanalyzed incidents.

But it seems, when we read [5], that the (justifiably) expected effect was that the quality of investigation directly affected the information fed back to reporters (as through

[2] That is, they rise and fall together

[3] This was discussed and resolved in personal communications with F.O. Sveen.

loop R1), thereby affecting reporter's motivation. This is not the case in the drawing presented. In the causal loop diagram, any effect on motivation comes from the fluctuations in the *number* of investigated reports, which sinks with reporting quality. This means that other factors affecting the number of reports, would have exactly the same effect on motivation. And so, the statement displayed in loop B4 would be that overworked investigators (insufficient resources) lead to a reduction in reporting *through less awareness in the organisation*, and not through a lack of motivation. The latter is merely a side effect.

To simulate any specific effect from inadequate resources, "Resources for Event Investigation" must directly affect "Evaluated and Disseminated Events & Incidents", or some other factor in loop R1. We spent a lot of time trying to understand how to deal with this problem. However, the IRS Model's creator, F. O. Sveen later explained that in the *simulation model* they have accounted for this. The causal loop diagram is slightly simplified, and that created this inaccuracy, which is merely an oversight. A more recent model by Sveen et al.[9], building on [5], has incorporated this kind of connection in the causal loop diagram, too.

Inherent in the loop is also the assumption that as resource contention increases all events will still be investigated at the same speed, only at lower quality. This assumption is also made in [9]. However in reality there would likely be significant delays in investigation, and events might well go uninvestigated. At a glance, this seems to have more or less the same effect, but it remains to be shown.

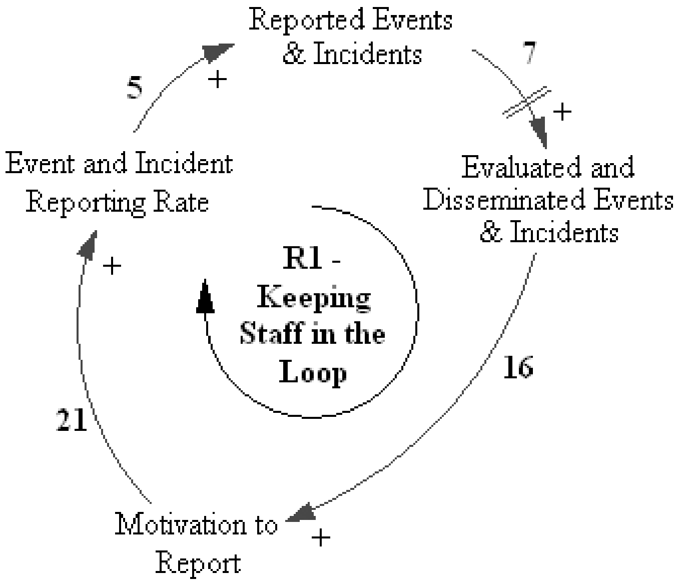

Figure 12: Loop R1: Keeping Staff in the Loop

Statement 26 *Keeping staff in the loop improves motivation*

(Loop R1, figure 12) As events and incidents are investigated, information about the results are fed back to reporters, and the organisation. As staff sees that the effort of reporting is fruitful, motivation to report increases, thus leading to further increase in reporting.

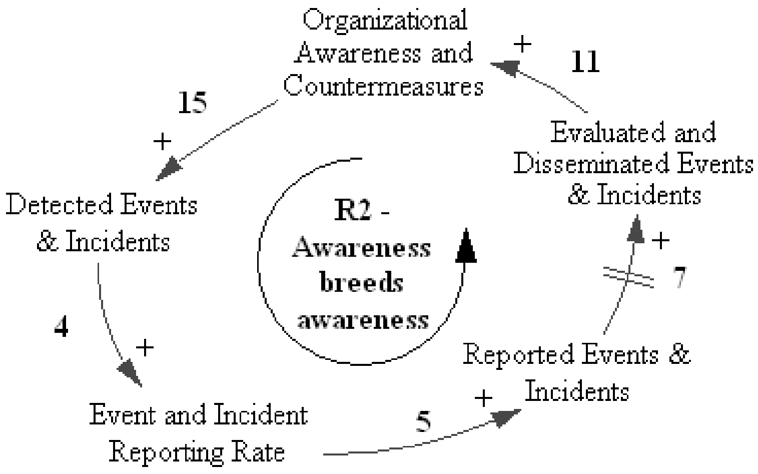
Organizational Awareness and Countermeasures
+
11
15
+
Evaluated and Disseminated Events & Incidents
Detected Events & Incidents
R2 - Awareness breeds awareness
+
7
4
+
Reported Events & Incidents
+
Event and Incident Reporting Rate
5

Figure 13: Loop R2: Awareness breeds Awareness

Statement 27 *Awareness breeds awareness (Safety Culture)*

(Loop R2, figure 13) We see that detected events lead to more reports, the investigations of which adds to the organisation's learning and knowledge. More knowledgeable, the organisation's awareness increases, further increasing its detection capability.

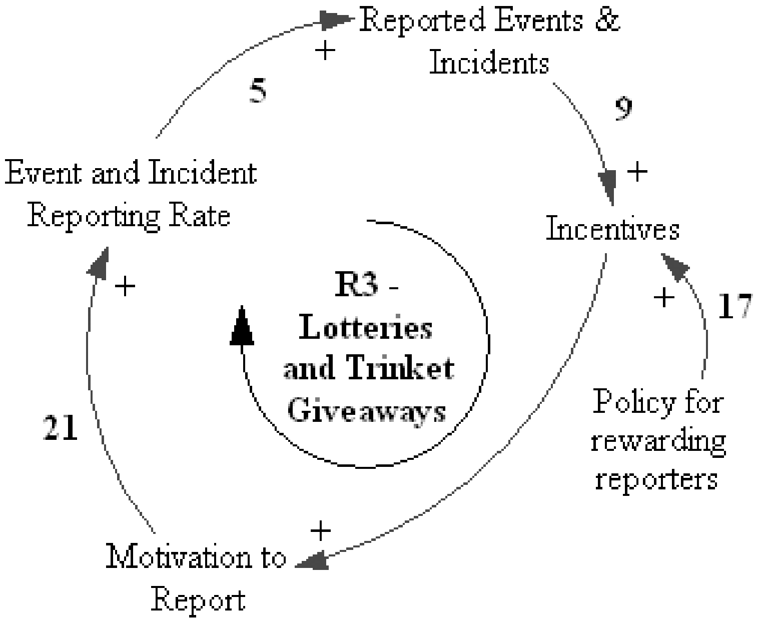
Reported Events & Incidents
+
5
9
+
Event and Incident Reporting Rate
Incentives
+
R3 - Lotteries and Trinket Giveaways
+
17
21
Policy for rewarding reporters
+
Motivation to Report

Figure 14: Loop R3: Lotteries and trinket giveaways

Statement 28 *Incentives improve motivation to report*

(Loop R3, figure 14) As noted under 17, if people are rewarded for reporting, the become more willing to report. Though initially beneficial, an unbalanced incentives programme could introduce biases in reporting. This is especially dangerous if combined with a culture of recriminations, in which serious events are likely to be underreported, something that would strengthen the bias towards reporting of less serious events.

6.6 Selecting hypotheses for closer scrutiny

After breaking down the model into statements, we joined forces with the other two aforementioned master's projects. With help from Finn Olav Sveen, who collected all three sets of model statements, a common superset was created. A simple vote (between all three students) on the 10 most important hypotheses to explore further, decided which direction we were to go in for the interviews. These 10 hypotheses were then rephrased and worded more generally, to suit all three projects, and be more easy to adapt into interview questions.

The resulting set of hypotheses we wanted to confirm or refute was:

Hypothesis 1 *Feedback to reporting staff and other relevant staff is necessary to motivate for reporting in the future. If staff does not see that their reports are helpful and are taken seriously they will not report in the future.*

Hypothesis 2 *Unclear guidelines and other insecurities regarding reporting of security events and incidents lead to sub-optimal reporting and thus sub-optimal learning. I.e. if staff do not know what to report, whom to report it to and how to report it, the organisation will not learn effectively.*

Hypothesis 3 *Lessons learned from investigations of incidents enable the organisation to raise awareness of security and put in place technical and organisational countermeasures that are effective in reducing future vulnerability. I.e. repetition of previous incidents and events should be reduced, attackers will be deterred from attacking and unintended security lapses, e.g. misplaced laptops, will be less likely to occur. Furthermore, attacks and unintended security breaches are detected and mitigated before they can cause substantial harm. In other words events do not escalate to attacks.*

Hypothesis 4 *Lessons learned from incident and event reports depend on the quality of investigation of reports. If work pressure is high; quality of investigations goes down as investigators cut corners to reach over all the work. Investigators prioritize the most important reports if resources are low, but even if investigators prioritize reports, less important reports still steal time and negatively impacts overall quality.*

Hypothesis 5 *Reports may be accompanied by recriminations such as disciplinary action, isolation by colleagues and so forth.*

Hypothesis 6 *Incentives are rendered ineffective in the presence of strong recriminations. I.e. they may lead to a bias in reporting towards "low-recrimination" incidents or towards no reporting at all.*

Hypothesis 7 *Events and incidents have similar causes.*

Hypothesis 8 *Near-miss (event) reporting is useful within information security.*

Hypothesis 9 *Top management support is crucial for the success of an information security reporting system.*

Hypothesis 10 *Staff will not comply with a reporting policy if they do not have time and competence, or see reporting as not useful.*

The next step was to create an interview protocol, or guide, to help us gather information to support or refute these hypotheses. We describe this in the next chapter.

7 Interviews / Case study

7.1 A change in conditions

As mentioned initially, the literature study part of this project turned out to be significantly larger than expected. This was in part, we have to admit, due to an initial underestimation of the scope, but also because we discovered new sources along the way, that we felt contained important insights, and deserved some attention. As a result, the interview part of the project was started later than planned. Unfortunately, in the very busy environment of the hospital we have visited, finding possible respondents, that were available in the remaining time, proved difficult. As a result, our initial goal of nine respondents was reduced to three. As described in chapter 4 we therefore changed the interview protocol so that all three respondents were asked the same questions. In our description of the interview questions below, we show which information was not collected as a result of this change.

7.2 Creating interview questions

After studying the IRS Model, and formulating hypotheses about it's behaviour (chapter 6), we subjected the ten hypotheses to a similar treatment as the statements that led to them. Each of the three master's student's wrote a proposed set of interview questions. The questions were discussed among the three, and with F. O. Sveen. Each proposal was then sent to Sveen, who merged them into one common set. Comments on the interview protocol were also sought from Eliot Rich[1], who has extensive experience in this kind of work.

Initially, the questions were set up in three similar, but slightly different groups, for different types of respondents. In practice only the "regular staff" set of questions was used. For comparison, the full set of interview questions is shown in the appendices.

We now turn to the description of each selected question:

Question 1 *Does your organization have an information security incident reporting policy?*

a. How were you made aware of this policy? (Training, written communication, at time of employment, etc.)

This question tells us something about what the interviewed person knows about the subject. Also it provides some information on to which extent there is a (mis)match between the information needs and actions in the organisation, and the actual information received and digested by staff. Pertains largely to Hypothesis 2, but also 1 and 10.

Question 2 *Have you received any form of guidelines, information or training in the use of the incident reporting system, how to recognize an incident and what to report?*

a. If so, to what extent?

[1] Assistant Professor in Dept. of Information Technology, University of Albany

This question has much the same basis as the previous, only with more focus on the reporting system, not just policy. With both questions, we want to obtain information that point to how much information staff members received, and actually picked up. We cannot from these questions alone determine how much information was "pushed" out to staff, since we are only asking what staff know (remember) that they have received. For information on what was actually, or supposed to be, delivered, we rely on communications with the hospital's IT-security manager and policies and guidelines made available to us. Discrepancies here could also be indicative of a non-functioning system, and to lack of managerial follow-up and implementation at least on lower levels in the organisation.

The following four questions were included to find out how the system appears to be working, from the staff's perspective. Particularly, we are interested in seeing to what extent information from the system is fed back into the organisation, and how this has affected information security and policies. The questions pertain mostly to hypotheses 1 and 3.

Question 3 *Is information about incidents that have occurred within the organization regularly made available to you?*
a. If so, in what way?

Question 4 *Please describe an incident that you, or a colleague, reported. How was the report followed up? What kind of feedback did you receive after you reported?*

Question 5 *Has information security improved after the introduction of a formal incident reporting process?*
a. Why/ Why not?

Question 6 *Do you know if policy has been changed as a result of incident reports?*

Turning to reporting culture, we would like to see how the use of the reporting system, and the enforcement of policies affects reporting. We hypothesise that incentives and recriminations have major effects on reporting, and would like to see how this matches staff's perceived reality. The following questions pertain to hypotheses 1, 5, 6, 8 (in part), and 10. We also ask specifically about top management commitment (hypothesis 9).

Question 7 *Please describe the reporting culture in your organization. Why is the reporting culture as it is?*

Question 8 *Have you or any of your colleagues been subjected to disciplinary action after you or any of your colleagues reported an incident?*
a. What do you think the effect of disciplinary action is?
b. How often is disciplinary action used?
c. While organisations often have official policies on the handling of incidents and reporting, it is not uncommon that reporters are subjected to hidden reactions from colleagues or managers. For instance, being passed over for promotions, or effectively frozen out of the workplace social environment, as a form of revenge for disloyalty. Do you know of, or have heard of situations where this has happened?

Question 9 *Are there any incentives for reporting security incidents?*
a. What do you think the effects of incentives are in this case?
b. How often are incentives used?

Question 10 *Does top management embrace incident reporting?*
a. Why do you think so?

Question 11 *What are the consequences of top management's attitude, and how important do you think it is?*

Question 12 *Do your superiors follow up the incident reporting system? Do they take an active interest?*

For the next to last question, we brought to discussion in the group (of 3 projects) whether it was actually necessary to focus spend time on this. Not that it is not important, however it is not necessarily so that this has special connections with information security or incident reporting. Instead, we undrestand this as a more general management issue, relating to how workers will prioritize tasks that are non-essential to daily operations, depending on managerial commitment to and focus on the task. We have not delved into management literature to conclude definetly on this by ourselves, though various of our sources, for instance [22], have included references on the subject. We base our a priori assumption of it's importance on these (for example, [22, ch. 10] talks a lot about organisational issues). The general importance on management commitment can also be easily argued from the fact that when it comes to prioritizing use of resources in the workplace, management have the final word. If they focus all resources solely on regular operational issues, then that is where the effort will be made. However, out of the interest in gauging the strength of management involvement at the hospital, we agreed that it was indeed an interesting question to ask.

7.3 "Lost" information

What is then not covered in the questions above is information on the effects of event vs. incident reporting, as well as the quality of reporting/investigations (hypotheses 4, partly 6 and 8). However, through conversation with the hospital's IT-security manager, we understood that they felt events and incidents were difficult to separate, and that this separation was not given much attention for reporting purposes. Which *consequences* they had in the end, though were widely different.

Also, we did not gather specific information on how the organisation perceives the causal relationships between event and incidents (hypothesis 7). The latter is conceived as needing of (at least) some in-depth knowledge of the subject, and was covered in a question for security personnel.

7.4 The hospital

We were fortunate enough to be allowed inside the doors at one of the larger Norwegian health care institutions, a hospital in the south-eastern region of Norway[2]. We decided in advance not to name the hospital, as part of the anonymisation of the interview respondents, and to be able to discuss any security issues that might surface, without fear of attracting negative attention to the particular hospital.

The hospital has several thousand employees (more than 4000). The organisation has an administrative division, an operational support divison[3], and several medical di-

[2] The public Norwegian health care sector is divided into geographical regions, regions South and East were merged into one in 2007

[3] janitorial services, backoffice, and other non-medical operational functions

visions.

All following information, unless otherwise noted, about security organisation, security issues and security measures, was obtained from the hospital's IT-security manager, in conversations or via email.

The hospital has always had to relate to safety issues (patient/medical), and the information security issues related to patient journals. As the use of IT in the hospital has increased, more and more attention has also been paid to IT-security. According to the IT-security manager, the hospital has a strong commitment to information security, well established in top management. This manifests itself in, for instance, the IT-security manager function reporting directly to top management, and the adoption of the "privacy ombudsman" role[38, §7-12], which is formally assigned to the IT-security manager.

The IT department of the hospital has implemented strong security measures to prevent unauthorised access to hospital computer systems from the outside of the hospital, as well as for control of employees use of IT-systems. Such measures are required by law (eg. [38]) to be strong enough to not be infeasible to circumvent. The hospital also adheres to a Code of Conduct for Information Security[58], that elaborates on issues concerning information security. The Code of Conduct is based on, and expands on, legislation that all health care institutions in Norway are required to follow[35, 38, 37, 57].

Main focus for reporting on information security issues, is related to the handling of patient information internally at the hospital. Specifically, the use of electronic patient journals is what raises the most issues. This also means that for most practical purposes, information security issues are increasingly also IT security issues.

The electronic patient journal system controls and logs all accesses to journals. Access is given on a need-to-know basis, that is, access is given only to those who need information in order to provide the necessary treatment / service. In practice, this involves giving access to the smallest possible set of journals (for instance, a nurse can get access to all patients in a ward), instead of to each individual journal. It is possible to override access controls to obtain necessary information, though the conditions under which this is allowed, and what personnel is authorized to do so, is strictly regulated.

The hospital has had an electronic reporting system for medical incidents for some time, but in the last year they have transitioned to a new system. The more modern system is available to all employees for reporting and lookup, and is also intended for information security reports, and not just medical incidents.

IT operations related issues are mostly handled internally in the IT-department and are registered in their operational incident handling system, unless considered having "very serious" consequences, or being direct breaches of established policies. Such incidents are reported further to the relevant managers (IT-, safety- or line-) for further follow up.

All employees must sign a statement to that they have read the hospital's security (and safety) instructions and policies. Failure to adhere to these policies are punishable, by official warnings in employee's file, and for very serious or frequent repeat occurences, by termination of employment (and possibly legal prosecution). While unauthorized access to or disclosure of information is an information security matter, and as such reported to security management, violation of policies/regulations is considered a personnel-/HR-matter. The handling of the issue, with respect to the involved staff members, is the responsibility of line- or HR-management. This includes, for instance, meetings with the involved staff members to establish what has happened, where there is suspicion of policy violations.

So the IT-security manager does not perform investigations into incidents beyond technical/IT-system matters. Any actions related to personnel management is performed by those with personnel management responsibilities.

The hospital defines "incident" as any happening that *indicates a possible violation* of policies / regulations. As such, the definition covers to an extent both events and incidents (as they are defined in this project), depending on the situation. Event vs. incident reporting, in the sense that this project discusses it, is thus not a consideration at the hospital.

7.5 Performing interviews

The interviews were performed one-on-one with each respondent. Two interviews were performed in the reposondents' own offices, the third was conducted via email. The first interview gave us some points of feedback on the questions, and questions 7 and 9 were changed as a result. In particular, 9c was initially poorly stated, and was perceived as offensive / not serious. It was edited to clarify that we were not looking for a hidden organisational policy of recriminations, but rather unofficial reactions that the organisation was not in direct control of. Interviews were scheduled to last about one hour each, but the average time used was about forty-five minutes.

7.6 Interview results

Below are summaries and discussions of the answers given during the interviews. To avoid complicating the text with constant references to "he/she", we name our respondents A, B and C. We try not to interpret the answers too much, since our group of respondents is so small. We do however try to give some possible explanations to some of the answers.

Question 1 *Does your organization have an information security incident reporting policy?*

a. How were you made aware of this policy? (Training, written communication, at time of employment, etc.)

Of the three respondents, two were familiar with current policies, and had been presented with policies and regulations (in writing). However, respondent C was *not* aware of any such policy, but assumed that one did exist. C could not recall having been shown any information security policy documents. No training is given on the subject, according to the IT-security manager, so no answers to that effect were expected.

We see a contrast here, to the claim that all employees must sign a statement to the effect that they have read said policies. In this case, an explanation could be found in that C has been with the hospital for many years, from before the current regulations existed. As such, the problem might be that existing employees were not expected to give this statement when new regulations were put in place.

Also, over the years, there might have been changes and reorganisation of institutions, and transfer of personnel between institutions. Perhaps there are no proper procedures in place to "update" the personnel affected, as they fall under these regulations.

Question 2 *Have you received any form of guidelines, information or training in the use of the incident reporting system, how to recognize an incident and what to report?*
a. If so, to what extent?

Again, respondent C (as the only one) answered negatively, but did point out that generally he/she would report work related issues to line management, and that this would be C's "reporting channel" also for information security, should the need arise.

One of the other respondents said that little information, and no training, was received, but that most knowledge and competence was attained through his/her personal initiative.

The third respondent said that (quote) *everyone receives basic training in the use of the incident reporting system*, and that various information was distributed through department meetings and other channels (such as Intranet).

The difference in answers between respondents, in part also for the previous question, could be explained by different positions in the organisation. For instance, one respondent said that the hospitals various divisions operate under a large degree of autonomy. As such, even if they have common policies to adhere to, they do not in reality share the same top level management, and possibly differ wildly in how operations are managed, on all levels. Also, depending on function, not all departments at the hospital deal with patient information (sensitive or not). Administration, janitors, cleaners, laboratory workers (to an extent), orderlies, and probably many others, are not (directly) involved in patient treatment. They should therefore not deal with, for instance, patient journals. For this reason, we would not be surprised to see that the emphasis on information security is less in certain departments.

Question 3 *Is information about incidents that have occurred within the organization regularly made available to you?*
a. If so, in what way?

All three respondents said no to that incident information is "pushed" out in general. However, A and B both said that information on serious, or high profile incidents (esp. if there is media coverage), or information on snooping in patient journals, is given through the Intranet and other internal hospital communications.

All incident reports are also available to all employees for lookup, through the reporting system. Managers can also use the system to get reports on incidents for their respective departments.

Question 4 *Please describe an incident that you, or a colleague, reported. How was the report followed up? What kind of feedback did you receive after you reported?*

Respondents told us of several incidents they knew were reported. For instance, two respondents pointed to a common problem: patient information left in pockets of clothes that are sent to the laundry, either on paper or sometimes even on computer memory sticks (which are not allowed to begin with). Feedback on these events primarily goes to the careless member of staff.

One respondent also said that in certain cases, feedback to the reporter was difficult, since the case information could involve a personnel matter. Consider, for instance, a case where someone reports a colleague for snooping in a journal. Since this is an HR / personnel issue, information on how the issue was resolved must remain confidential.

Respondents also knew of cases where patient information was wrongfully sent to laboratories through the pneumatic tube system[4]. One respondent also referred to an incident where patient information was sent, in a taxi, between two health care institutions. In a hurry, the taxi driver proceeded to hand the package of (visible) information to a random employee at the hospital, requesting the person to deliver it to it's intended receiver. This incident was reported, but the reporter never heard about it again.

Question 5 *Has information security improved after the introduction of a formal incident reporting process?*
a. Why/ Why not?

A and B, both familiar with the reporting system, answer positively to this effect. Respondent A felt that with the new system, reporting and getting (ie. finding) feedback was made much easier, and that this implicitly had a positive effect. Respondent B viewed improvements in information security more as a long term achievement through focus on security, of which reporting was only one part. The hospital's focus on reporting and the subsequent handling on snooping incidents, B said, has raised awareness to the importance of security.

Question 6 *Do you know if policy has been changed as a result of incident reports?*

Respondents said policies had not been changed as a direct consequence of reports, instead they evolve as the organisation develops and changes over time. Procedures have changed though, as a result of audits. One department had received an audit remark for poor identification procedures when disclosing patient information over the phone. This had led to better checks of callers identity, and better control of what information was disclosed.

Question 7 *Please describe the reporting culture in your organization. Why is the reporting culture as it is?*

Again, it was pointed to that the hospital's many divisions, in themselves fairly large organisations, were probably different in this respect. "*Likely, there are many reporting cultures, not* **a** *reporting culture at the hospital*", said respondent C.

[4] The pneumatic tube "mail" system is a traditional form of transport for papers, and in recent years, for lab specimens, in hospitals. See for instance www.swisslog.com, a large supplier of such systems.

Respondent B felt that the already well established culture for medical incident reporting also laid the ground for information security reporting. "*There is an open attitude that mishaps should be reported, and learned from*", B said.

Respondent A felt that the reporting culture was still lacking, even if reporting was made easier with the new reporting IT-system. Underreporting is still a problem. A said that (perceived) insignificant, minor incidents were seldomly reported, especially if they were resolved on the spot. "*If the issue was resolved, why waste more time on it?*", was seen as a common attitude, especially since staff ususally have their hands full just doing their regular work, if they were not to be burdened with extra reporting as well. There was seldom much thought given to that it might be useful to report minor incidents. More serious incidents, however, their department was quite good at reporting, was A's impression.

Question 8 *Have you or any of your colleagues been subjected to disciplinary action after you or any of your colleagues reported an incident?*

a. What do you think the effect of disciplinary action is?

b. How often is disciplinary action used?

c. While organisations often have official policies on the handling of incidents and reporting, it is not uncommon that reporters are subjected to hidden reactions from colleagues or managers. For instance, being passed over for promotions, or effectively frozen out of the workplace social environment, as a form of revenge for disloyalty. Do you know of, or have heard of situations where this has happened?

Respondent B knew of cases where action had been taken, in relation to journal snooping. Respondents A and C did not know of specific incidents, but A had heard of it happening at the hospital.

One respondent did not think that disciplinary actions would be relevant in his/her department, since they generally did not deal with sensitive information. Another respondent thought it would have a negative effect on reporting. The third respondent felt that the threat, and use, of disciplinary actions had helped improve the awareness and understanding for how serious security must be taken.

As to hidden reactions, respondents A and C both replied that they had heard of it happening, in relation to medical mishaps, but not information security. Particularly, among doctors there is (supposedly) a fear of reporting mistakes and errors. Some, it was said, are afraid to tell colleagues in a very competitive environment, others could be afraid of telling due to the possibly serious consequences that treatment errors can have. One respondent had also heard that other staff had complained to being passed over for promotions, or being subjected to subtle recriminations from colleagues.

Respondent B did not know of any such happenings (in relation to information security). B felt that the open culture of learning from mistakes, adopted from the medical reporting culture, put a positive spin on reporting, and thus precluded such behaviour.

Question 9 *Are there any incentives for reporting security incidents?*

a. What do you think the effects of incentives are in this case?

b. How often are incentives used?

None of the respondents could point to incentives being used to promote reporting, except for the inherent motivation in the attitude that reporting is done for the sake of improvement.

Question 10 *Does top management embrace incident reporting?*
a. Why do you think so?

Respondents B and C both felt that top management was genuinly and deeply committed to incident reporting, as part of the security and safety culture. Respondent C pointed to the establishment of a system/process for anonymous reporting, with specific contact points and clearly specified handling rules for reports. C felt that management embraced this control mechanism that allowed them to discover adverse incidents that might not be picked up through regular "chain-of-command", and that this was founded in management's genuine interest in the quality of the hospital's services.

Respondent A did not feel this in the same way, and did not have the impression that it was an active issue at top management level, except for mandatory tasks/reviews. At the lower levels of the organisation, they never heard from divisional management (for instance) in these matters.

Question 11 *What are the consequences of top management's attitude, how important do you think it is?*

Respondent B did not reply to this. Respondents A and C both recognized the importance of sustained top management commitment, to maintain commitment at lower levels of the organisation. *If top brass do not require it, it won't happen,* A said. C felt that even if top management was commited, it seemed difficult to communicate this commitment to the rest of the organisation. There were at least two reasons for this, C reckoned: first that the autonomy of each division somewhat separated hospital top management from divisional top management, and that staff in the various divisions in reality related to the latter. Second, as you move down in the organisational hierarchy, you "loose" managerial compentence and gain professional / operational skills. With this loss, some of the understanding for performing administrative tasks, and tasks like incident reporting, was lost. C pointed out, though, that the hospital had started a training programme for lower level (first-line) managers, in order to raise the management competence level for these managers. This was hoped to counter for some of this loss of management understanding.

Question 12 *Do your superiors follow up the incident reporting system? Do they take an active interest?*

Respondent A said that reporting was usually mentioned in passing at mandatory, yearly management reviews. It was usually the last point on the order of the day, and was not given much attention. B said that serious incidents were brought to (top) management's attention, where gravity of the incidents so required. C did not answer this question.

We shall now return to discussing how the IRS Model fits into information security, before comparing it to our interview findings.

8 Incident reporting, The IRS Model and Information Security

When we started this project, it was after reviewing the IRS Model paper[5] only. With idealist optimism we were certain that this had to be unconditionally suitable for information security reporting. As we dug deeper into the literature, however, our view attained more nuances. We still believe the model generally suitable, but we now recognize some of the differences between safety and information security (IS) events and incidents.

All things considered, we see the model as a good starting point, but somewhat "unfinished" with respect to information security. Our ideas are not all confirmed through literature alone, but would require simulations to validate.

When we now seek to answer our research questions, we will mostly discuss the first two together, as we feel the arguments are tightly connected.

We asked:

Question 1 *Can incident reporting be a useful tool for improving information security?*

Question 2 *Can the IRS model be used within information security?*

Question 3 *How does the IRS model correspond to a real life ISIRS?*

Our conclusion on question 2 is positive, and inherent in this is is our expectation that the reporting actually is useful. The third question is covered in a separate section.

8.1 Safety Events and Information Security incidents

As we have mentioned, Sveen et al[9] (not quite the same group of authors as in [5]), have also built on the general IRS Model for information security. We adopt a slightly different angle to this, than they do. In [9] information security and computer security are considered the same. In most contexts this is true, as we have ourselves hinted at in the introduction. However, when focusing solely on computer security incidents puts ut at risk of loosing a whole range of incidents. Let us look at the different types of information security incidents and events that we expect to find, particularly within our our health care case:

- Insiders accessing information without authorization, by mistake.
- Insiders accessing information without authorization, deliberately.
- Externals accessing information without authorization, by mistake.
- Externals accessing information without authorization, deliberately.
- Insiders disclosing information to unauthorized third party, by mistake.

- Insiders accessing information to unauthorized third party, deliberately.

As events, we consider *attempts* at doing any of the above. As incidents, we consider *successful execution* of any of the above. If we focus solely on computer related incidents (and events), we will miss all those occasions where information is handled on paper or verbally, which might just as well happen in all cases above. For instance, a typical problem at the hospital, as we were told during the interview, is journal printouts that are left in jacket pockets when these are sent to the laundry.

So, at least for our health care case, non-computer events are just as important as computer-related events, even though they might be much smaller in numbers (with increase in computer use).

The IRS Model relies heavily on the relationship between events and incidents. It seems that, in the available literature, event (often termed near-miss) reporting is promoted for two reasons, both to help find and eliminate causes for more serious incidents. The first reason is the claim that events and incidents have the same underlying causes [20, 21, 22, 24], and the second, that events can/will lead to incidents[5, 28, 31]. Even if [24] support this thinking (though in terms of "minor" and "major" events, this still leaves the question of whether there is a link between the minor and major events, or their causes.

Intuitively, there should be (for instance, if you are careless/sloppy in nature, it would be common sense to guess you are more likely to end up in a serious accident), but is there any actual evidence of this? Johnson quotes sources that support both theories, and the question remains unanswered.

We are not convinced that the link between events and incidents is as strong in an information security context. For instance, we expect that a majoriy of incidents will be computer related. We assume here that most computer systems are robust enough, software bugs excempted, that a repeat attempt at accessing information, under the same conditions, will not yield a different result than in the first attempt. Two thought up examples illustrate the point:

- (1) At an industrial plant, multiple near-miss reports are filed for slips/trips. Many workers have slipped on the same spot of floor, but noone has so far been injured. One day, a worker slipped in the same spot, but was ufortunate enough to hit his head when landing, the event (slipping) suddenly escalating into an incident (or accident). Could it have been predicted and prevented?
- (2) An it-system security log reports multiple (failed) break-in attempts to a publicly available service on the Internet (for instance a web page). Such events are to be expected in today's Internet, and firewalls and servers are commonly configured to withstand all known and anticipated attacks. The options are to take the service offline, or to accept that it will be a target. One day, a successful break-in is performed, and the incident report reveals that a change in configurations lead to a weakened defence. Could it have been predicted and prevented?

In the first case, the answer is a clear yes. This was a definetly "an accident waiting to happen", and is an example of an event that is unexpected and unwanted and reporting should have lead to mitigating action. The second case is trickier, though. Here the events were expected, and however unwanted, their origin was completely outside of the system owner's control. Event reports only confirmed that the defences worked as expected, and that there was no reason to expect an escalation into a break in (that an incident could occur). It took a change in the system to make the incidnet possible. In both examples, the event and incident were identical happenings, except for the outcome, but only in the first example could the event be counted a (predictive) precursor. It is the change in the it-system that is the precursor / predictive event here, but such events are relatively few in numbers (e.g. compared to firewall logs of illegal network traffic).

Care must be taken then, when building (or modelling) an IRS for information security (ISIRS), to ensure that causal relationships between events and incidents are not overstated, and that the system allows for types of events where this relationship might not exist.

This is not to say that predictive events do not exist in information security. For instance, events that point to a poorly constructed work procedure, perhaps to lax in controls and allows for too much error, would be good predictive or precurson events. At some point, someone will likely slip through a hole in the procedure, deliberately or by accident. We just think that in a world of so many computer systems producing logs that are to be audited and watched (see for instance [38, 37]), the amount of non-predictive events as described above, would overshadow predictive ones. To avoid this, better (smarter) systems must be put in place, but today it is still a problem for institutions like CSIRTs[41, 42].

This is, of course a known problem of reporting systems: If they swamp the operator, they will not be effective. in fact they might even reduce security of safety, as they would not produce output that is relevant to the input received. This could lead to erroneous status reports for security.

It is not only an increase in real incidents and threats that would contribute to this, but with ever increasing use of computer systems, there is also increasing use of automated incident detection systems, such as Intrusion Detection Systems (IDS). Computers perform vast numbers of operations for even the most mundane tasks, and accordingly these detection systems handle an enormous amount of "normal events", and suffer from the *base rate fallacy* [60, pp. 77-78]. This can easily cause a system to be overflowed with false positives, ie. reports on incidents that turn out not to be incidents after all.

As mentioned about our hospital's patient journal system, access is given on a group-of-journals basis. Controlling acces for every person to every individual journal would simply be prohibitive. Not only would it cause a lot of administrative overhead just to manage access, but imagine the alarms that would go off, likely constantly, when people tried to access information they needed, for which the acces controls system wasn't quite updated on at the time.

To sum up, we suggest that the realtionship between causes of events and incidents, is not a strong in information security as in safety. Also, we do not believe that there is (universially) a link between event and incident causes. The latter would also impact the effect that learning from events would have on incident occurence.

8.2 Deliberate events and incidents

Another difference between safety and information security, is that there are much more events (and incidents) of deliberate nature, than there are in safety. Safety reporting literature revolves around terms like near-misses, mishaps, accidents, etc. feeding a notion of being unfortunate, but not deliberate happenings.

For information security, we deal a lot more with deliberate events, like our hospital that deals a lot with snooping in patient journals. Or, like our example above of external assailants hammering away on our internet-exposed computer systems.

There is something here that affect the IRS Model, as it stands today. First, we must lower our expectation for what effect awareness has on event and incident occurence. This is due to the nature of the deliberate assailant. We dare assume he is well aware that he is breaking the rules. As such, telling him it is bad, and that he should not do it, will have little effect. Countermeasures to prevent possibilities for such events could of course still be developed through this learning, but the effect is still reduced. From an insider, a staff member who is trusted with certain information, it might not be possible to protect oneself. He has necessary access to information through his daily work, and if he chooses to abuse that information, there is little that can be done to stop him[1].

Secondly, another factor that contributes to this, is the introduction of the external assailant or attacker. The argument is largely the same: learning can help build contermeasures, but won't build awareness or better attitudes in hackers across the globe..

And so, we claim that there is a reduced effect of awareness on event/incident occurence in an information security IRS, compared to a safety IRS.

8.3 The IRS Model simulations

Simulations using the IRS Model, have shown that its behaviour corresponded with for instance the results of Nielsen et al.[20]. The most interesting conclusion from [20] is perhaps that there is a correlation between apparent[2] top-management commitment and improvements in safety. This is precisely one of the points effectively made by Sveen et al, where their model mandates policies to encourage reporting, and not the least to spend resources on a complete organisational learning system for information securit. (These are typically top management, organisation-wide decisions.)

Still, conditions for the simulation runs are idealized, and all the presented scenarios are somewhat "black and white". Lessons learned from simulation runs range from the seemingly obvious ("Punishment demotivates people") to more subtle relationships between reporting rates and perceived security and underreporting. We would like to

[1] Except thought control, maybe?

[2] Apparent, since it is measured from the viewpoint of workers.

see more simulations for varying parameter combinations, but from what we have learnt from the incident reporting literature, and given our thought on variations/changes in model assumptions (these assumptions are manifested as parameters in the simulations) we find the model credible, and as such useful for information security reporting.

8.4 On the usefulness of reporting

Johnson[24] argues that IR is cheaper than accidents, in a safety context. This might be well documented for the health, safety and environment field, but empirical documentation for this is hard to find for information security. In Norway we have, at best, estimates based on few and limited sources (I.e. Mørketallundersøkelsen, The Dark Figure survey[3]). The survey shows that information security (or IT-security, specifically) incidents already incur substantial costs to norwegian businesses.

As legislation demanding stronger information security is put into place, eg. with the introduction of the Sarbanes-Oxley Act [36] in the USA and it's cousin "EuroSOX" [62] in the EU, it is not far fetched to accept that Johnson's argument is valid also for information security[4], at least for businesses. Stronger legislation is also evolving for the (public) health care sector, as we have seen earlier.

Theoretical research on the value of information security investment does exist[63], but we know little of calculations on the economy of incident reporting for information security.

Money spent is not the only issue when discussing usefulness. Kjellén[22] refers to Argyris[64], and warns that the *SHE information system* (of which our incident reporting would be part) must be used as a problem-solving tool, involving the entire organisation. Particularly, he highlights that there is a limitation imposed by management receiving aggregated information upon which to found operational decisions. Given this limitation, decisions as to remedial actions (following an investigation) should be made at as low a level as possible. This requires that the information in the event reporting system is fed back "down" and into the system's lower levels, for instance supervisor or mid-level mgtmt. At the same time, trends and overall direction can be best viewed at the top level. Kjellén[22] cites Van Court Hare[65]: "For an analyst to gain control over a system, he must be able to take at least as many distinct actions [..] as the system can exhibit." (Ashby's law of requisite variety. I.e. at a lower level in the system (worker level), there are many more factors to control. For top-level management, factors and data are aggregated. Since the picture is less complex, so can control actions be. It is then simpler to make (general) decisions on a higher level, in order to influence (complex) system behaviour at the lower level.

We read this as an argument that top (or at least high level) management commitment is crucial to incident reporting usefulness, and that without such involvement, the whole system would be pointless.

[3] Mørketallsundersøkelsen 2006[61], by Næringlivets Sikkerhetsråd, a security organisation for Norwegian enterprises. A summary, in Norwegian, is available at http://www.nsr-org.no/artikler/morketall2006.htm. Copies of the report can be ordered from nsr@nso.no.

[4] Legislative demand supports two arguments for IR: (1) One must have it, it's the law, and (2) It's more expensive to ignore (1), and hope for the best, than to implement IR in the first place (given that authorities actually punish violators). There's no reason to think some businesses are not going to try to break these laws, any less than other laws.

8.5 The IRS Model and the hospital case study

Our foundation for saying anything about this is weak, due to the low number of interview respondents. We must thus bear this uncertainty in mind when evaluating the accuracy of our conclusions below.

Also, we were not able to gather information on all issues that we planned. For instance the questions particular to policy makers, and to security personell were excluded, foiling our discussion on the perceived importance of event (vs. incident) reporting.

However, we did see that the respondents expressed opinions that agreed to a certain extent with the asusmptions in the model. For instance, the importance of an open, non-punishing culture was recognized by all three respondents. As was the assumptions on the importance of top mangement commitment.

The fact that the hospital's policies did not always seem to support this, is another matter. So, even if respondents did agree with our assumptions, we did not perceive that actual system matched the IRS Model, on some accounts. Particularly this applied to the assumption on the negative effects on recriminations. It was claimed that they had seen positive effects from the policies of recriminations, countering the arguments of Sveen et al[5] and others. The hospital did not have any specific estimates on underreporting, though, and it is as such diffcult to attempt to gauge the actual effectiveness of their system.

Respondents (two out of the three) also gave the impression that training, and post-reporting organisational learning was not set up to a large extent in the hospital. Whether this is true or not, we cannot say for sure, as we do not know whether this was only the perceived reality of these two, or whether it is true in genral. And if it were true, the mechanisms of the model would then be somewhat different from the hospital's system, and the two would not be directly comparable.

However, one of the respondent did say that such mechanisms were in place. We see no reason that this person should lie about this, so if we accept that as a truth, the reason for the other two respondents' answers could lie in to little emphasis on the organisational learning, either a problem in the design of the system, or perhaps in a lack of management commitment.

This last argument, together with the impression that respondents answers agreed with some of the assumptions built into the questions, lead us to think that the IRS Model matches the real world system *to a certain extent*, but the result is in reality inconclusive.

9 Conclusion and future work.

We conclude that the IRS Model is definetly useful for information security reporting, albeit we presume it needs some tweaking of parameters to be adapted to such a setting. As such, only simulation results would confirm our suspicions, and we would suggest that future work on this model do precisely that: simulate more conditions that are better suited for information security reporting, for isntance as described in this report.

A Main aspects of the qualitative research interview

This listing was extracted from Kvale[7]:

- **Life-world**. The subject at hand is (part of) the interviewees everyday world, including his or hers own relationship to it.

- **Meaning**. The interview has as its goal to interpret the meaning of central themes in the interviewees life-world. The interviewer registers and interprets the meaning of what is said, and how it is said.

- **Qualitative**. The interview seeks to gather qualitative knowledge, expressed in common language. It does not attempt to quantify.

- **Descriptive**. The interview tries to collect open, nuanced descriptions of different aspects of the interviewees life-world.

- **Specificity**. Descriptions of specific situations and hendelsesforløp are collected, not general opinions.

- **Willful naivité**. The interviewer is open to new and unexpected fenomena, and avoids ready-made categories and interpretations.

- **Focus**. The interview focuses on specific subjects; neither tightly structured med standardised questions, nor completely unmanaged.

- **Ambiguity**. The interviewees statements can sometimes be ambiguous, which can reflect contrasts in his life-world.

- **Change**. The interviewprocess can give new insights and consciousness, and the interviewee can, during the interview, change his descriptions and interpretations on a subject.

- **Sensitivity**. Different interviewers can promote different statements on the same subject, depending on their sensitivity towards, and knowledge on the subject.

- **Interpersonal communication**. The knowledge that is collected is produced through an interpersonal interaction in the interview situation.

- **Positive experience**. A successful research interview can be a valuable and enlightening experience for the interviewee, who might gain new insight into his own life-world.

B Interview questions, complete set

B.1 Policy makers (managers and process owners)

Question 1 *Does your organization have an information security incident reporting policy? Please elaborate.*

a. Why do you / do you not have such a policy?

Question 2 *Please describe how incident reports are gathered and handled.*

a. Who does the investigation? Is there a dedicated team?

Question 3 *Does the reporting policy also include events?*

a. Do you think event reporting is useful? Why is this so?

Question 4 *Have guidelines been developed to inform users of the incident reporting system and process?*

a. Have the users received any form of training in the use of the incident reporting system, how to recognize incidents and what to report?

i. Why / why not?

ii. To what extent?

Question 5 *Is information about incidents occurring within the company regularly made available to users?*

a. Why / why not?

Question 6 *Do you keep the reporting users informed of the situation and the investigation of the incident report? Do the reporting users receive any information upon the closure of the incident investigation?*

a. Why / why not?

Question 7 *Is there any post-resolution follow-up of reported incidents?*

a. By whom? Why?

Question 8 *Has information security improved after the introduction of a formal incident reporting process?*

a. Why has it improved / not improved?

Question 9 *Has policy been changed as a result of incident reports?*

a. Why / why not?

Question 10 *Please elaborate on the reporting culture in your organization. Why is the reporting culture as it is?*

Question 11 *Traditional safety reporting systems are often plagued by underreporting. How is the situation in your organization? Please elaborate.*

a. Why is the situation like this?

Question 12 *Does the information security policy or information security reporting policy (or equivalent) include any form of disciplinary action?*

a. Why / why does it not include disciplinary action?

b. What do you think the effect of disciplinary action is?

c. While organisations often have official policies on the handling of incidents and reporting, it is not uncommon that reporters are subjected to hidden reactions from colleagues or managers. For instance, being passed over for promotions, or effectively frozen out of the workplace social environment, as a form of revenge for disloyalty. Do you know of, or have heard of situations where this has happened?

Question 13 *Does the information security policy or equivalent include any form of incentive for reporting security incidents?*

a. Why does the reporting policy include / not include incentives?

Question 14 *Do you personally follow up the incident reporting system or is this delegated to a subordinate?*

a. Why / why not?

Question 15 *Do your superiors follow up the incident reporting system? Do they take an active interest?*

B.2 Security personnel

Question 1 *Does your organization have an information security incident reporting policy? Please elaborate.*

Question 2 *2) Please describe how incident reports are gathered and handled.*

Question 3 *3) Does the reporting policy also include events (and not just incidents)?*

a. Do you think event reporting is useful? Why is this so?

b. Can anything be learned from events to prevent future incidents?

Question 4 *Have guidelines been developed to inform users of the incident reporting system and process?*

a. Have the users received any form of training in the use of the incident reporting system, how to recognize incidents and what to report?

i. Why / why not?

ii. To what extent?

Question 5 *Is information about incidents occurring within the company regularly made available to users?*

a. Why / why not?

Question 6 *Do you keep the reporting users informed of the situation and the investigation of the incident report? Do the reporting users receive any information upon the closure of the incident investigation?*

a. Why / why not?

Question 7 *What is the workload of those responsible for security incident investigation?*

a. Who detects most of the incidents / events? Automated sources (antivirus, firewall, etc.) or users?

b. How does the workload impact the quality of investigations? Please elaborate.

Question 8 *Is there any post-resolution follow-up of reported incidents?*
a. By whom? Why?

Question 9 *Has information security improved after the introduction of a formal incident reporting process?*
a. Why has it improved / not improved?

Question 10 *Has policy been changed as a result of incident reports?*
a. Why / why not, do you think?

Question 11 *Please describe the reporting culture in your organization. Why is the reporting culture as it is?*

Question 12 *Traditional safety reporting systems are often plagued by underreporting. How is the situation in your organization? Please elaborate.*
a. Why is the situation like this?

Question 13 *Does the information security policy or information security reporting policy (or equivalent) include any form of disciplinary action?*
a. What do you think the effect of disciplinary action is?
b. How often is disciplinary action used?
c. While organisations often have official policies on the handling of incidents and reporting, it is not uncommon that reporters are subjected to hidden reactions from colleagues or managers. For instance, being passed over for promotions, or effectively frozen out of the workplace social environment, as a form of revenge for disloyalty. Do you know of, or have heard of situations where this has happened?

Question 14 *Does the information security policy or equivalent include any form of incentive for reporting security incidents?*
a. What do you think the effects of incentives are in this case?
b. How often are incentives used?

Question 15 *Does top management take an active interest in the information security reporting system?*
a. What are the consequences of top management's attitude and how important do you think it is?

B.3 Regular staff

Question 1 *Does your organization have an information security incident reporting policy?*
a. How were you made aware of this policy? (Training, written communication, at time of employment, etc.)

Question 2 *Have you received any form of guidelines, information or training in the use of the incident reporting system, how to recognize an incident and what to report?*
a. If so, to what extent?

Question 3 *Is information about incidents that have occurred within the organization regularly made available to you?*
a. If so, in what way?

Question 4 *Please describe an incident that you, or a colleague, reported. How was the report followed up? What kind of feedback did you receive after you reported?*

Question 5 *Has information security improved after the introduction of a formal incident reporting process?*
a. Why/ Why not?

Question 6 *Do you know if policy has been changed as a result of incident reports?*

Question 7 *Please describe the reporting culture in your organization. Why is the reporting culture as it is?*

Question 8 *Have you or any of your colleagues been subjected to disciplinary action after you or any of your colleagues reported an incident?*
a. What do you think the effect of disciplinary action is?
b. How often is disciplinary action used?
c. While organisations often have official policies on the handling of incidents and reporting, it is not uncommon that reporters are subjected to hidden reactions from colleagues or managers. For instance, being passed over for promotions, or effectively frozen out of the workplace social environment, as a form of revenge for disloyalty. Do you know of, or have heard of situations where this has happened?

Question 9 *Are there any incentives for reporting security incidents?*
a. What do you think the effects of incentives are in this case?
b. How often are incentives used?

Question 10 *Does top management embrace incident reporting?*
a. Why do you think so?

Question 11 *What are the consequences of top management's attitude, and how important do you think it is?*

Question 12 *Do your superiors follow up the incident reporting system? Do they take an active interest?*

Bibliography

[1] Halttunen, K. 1983. *Confidence Men and Painted Women: Study of Middle Class Culture in America, 1830-1870*. Yale University Press.

[2] IBM. Ibm archives 1956. http://www-03.ibm.com/ibm/history/history/year_1956.html, last visited on Oct 29. 2007.

[3] Lawton, G. 2006. Working today on tomorrow's storage technology. *IEEE Computer*, 39(12), 19–22.

[4] Hollaar, L. A. 2002. *Legal Protection of Digital Information*. BNA Books.

[5] Sveen, F. O., Rich, E., & Jager, M. 2007. Overcoming organizational challenges to secure knowledge management.

[6] Neumann, W. L. 2000. *Social Research Methods - Qualitative and Quantitative Approaches*. Allyn & Bacon, 4 edition.

[7] Kvale, S. 1997. *Det kvalitative forskningsintervju*. Gyldendal Akademisk, Original title: Interviews. An introduction to Qualitative Research Interviewing.

[8] Ragin, C. 1993. *Constructing social research*. Pine Forge Press.

[9] Sveen, F. O., Sarriegi, J. M., Rich, E., & Gonzalez, J. J. 2007. Toward viable information security reporting systems. In *Proceedings of the International Symposium on Human Aspects of Information Security and Assurance*.

[10] Forrester, J. W. 1958. Industrial dynamics: a major breakthrough for decision makers. *Harvard Business Review*, 36 No 4, 37–66.

[11] Sterman, J. D. 2000. *Business Dynamics: Systems thinking and modelling for a complex world.* Irwin McGraw-Hill, Boston.

[12] Senge, P. M. 1990. *The Fifth Discipline: The Art and Practice of the Learning Organization.* Doubleday, New York.

[13] Wolstenholme, E. F. 2004. Using generic system archetypes to support thinking and modelling. *System Dynamics Review*, 20(4), 341–356.

[14] Marais, K. & Leveson, N. G. Archetypes for organisational safety.

[15] Wolstenholme, E. F. 2003. Towards the definition and use of a core set of archetypal structures in system dynamics. *System Dynamics Review*, 19, 7–26.

[16] Rich, E. & Gonzalez, J. J. 2006. Maintaining security and safety in high-threat e-operations transitions.

[17] Gonzales, J. J., Qian, Y., Sveen, F. O., & Rich, E. 2006. Helping prevent information security risks in the transition to integrated operations. *Telektronikk*, (1), 29–37.

[18] Gonzalez, J. J. 2005. Towards a cyber security reporting system - a quality improvement process. In *SAFECOMP*, Winther, R., Gran, B. A., & Dahll, G., eds, volume 3688 of *Lecture Notes in Computer Science*, 368–380. Springer.

[19] Gonzalez, J. J. Modelling security with system archetypes. Lecture notes in Security Management, Gjøvik University College, March 2006.

[20] Nielsen, K. J., Carstensen, O., & Rasmussen, K. 2006. The prevention of occupational injuries in two industrial plants using an incident reporting scheme. *Journal of safety research*, (37), 479–486.

[21] Jones, S., Kirchsteiger, C., & Bjerke, W. 1999. "the importance of near miss reporting to further improve safety performance". *Journal of Loss Prevention in the Process Industries*, 12, 59–67.

[22] Kjellén, U. 2002. *Prevention of Accidents Through Experience Feedback*. Taylor & Francis e-Library.

[23] Heinrich, H. W. 1959. *Industrial accident protection - A scientific approach*. McGraw-Hill, New York, 4 edition.

[24] Johnson, C. W. October 2003. *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*. University of Glasgow Press, Glasgow, Scotland.

[25] Huldt-Nystrøm, E. 2006. Registrering av uønskede hendelser: Utfordringer. *Oss i mellom*, (2), 13. Internal newsletter for Sørlandet Sykehus (Sørlandet Hospital), Norway.

[26] Fonneland, I.-L. 2005. Avviksregistrering ved intensivavdelingen, ssa. *Oss i mellom*, (2), 6. Internal newsletter for Sørlandet Sykehus (Sørlandet Hospital), Norway.

[27] Cooke, D. L. & Rohleder, T. R. 2006. Learning from incidents: from normal accidents to high reliability. *System Dynamics Review*, 22(3), 213–239.

[28] Tamuz, M. Understanding accident precursors. Technical report, National Academy of Engineering, July 2003. Lecture at workshop: Linking Risk Assessment with Risk Management.

[29] Cooke, D. L. 2003. A system dynamics analysis of the westray mine disaster. *System Dynamics Review*, 19(2), 139–166.

[30] Wallace, B. & Ross, A. 2006. *Beyond Human Error: Taxonomies and Safety Science*. CRC Press, Taylor & Francis Group.

[31] Sonnemans, P. J. M., Körvers, P. M. W., Brombacher, A. C., van Beek, P. C., & Reinders, J. E. A. 2003. Accidents, often the result of an "uncontrolled business process" - a study in the (dutch) chemical industry. *Quality and Reliability Engineering International*, 19(3), 183–196.

[32] Chapman, P. & Underwood, G. 2000. Forgetting near-accidents: the roles of severity, culpability and experience in the poor recall of dangerous driving situations. *Applied Cognitive Psychology*, 14(1), 31–44.

[33] ISO. 2007. *ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management*. ISO / IEC.

[34] SN. 1991. *NS5814: Requirements for risk analysis*. Standard Norge (Norwegian body of standardisation).

[35] Helse- og omsorgsdepartementet (Norwegian Department of Health). *Lov om helseregistre og behandling av helseopplysninger (Law on registration and use of health information)*, 2001. Available from www.lovdata.no. Last viewed Oct. 30. 2007.

[36] U.s. 107th congress. 2002. HR3763, An act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes (Sarbanes-Oxley Act).

[37] Justis- og Politidepartementet (Norw. Dept. of Justice). *Lov om behandling av personopplysninger (Personal Data Act)*, 2000. Available from www.lovdata.no. Last viewed Oct. 30. 2007.

[38] Datatilsynet (The Norwegian Data Inspectorate). *Forskrift om behandling av personopplysninger (Personal Data Regulations)*, 2000. Available from www.lovdata.no. Last viewed Oct. 30. 2007.

[39] Common criteria project. the official website of the cc project. http://www.commoncriteriaportal.org. Last visited Oct 30. 2007.

[40] Stoneburner, G. August 2006. Towards a unified security/safety model. *Computer*, 96–97.

[41] Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. Organizational models for computer security incident response teams. Handbook CMU/SEI-2003-HB-001, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA, USA., 2003.

[42] Wiik, J., Gonzalez, J. J., & Kossakowski, K.-P. 2005. Limits to effectiveness in computer security incident response teams. In *23rd International System Dynamics Conference, Boston, Mass., USA*.

[43] Paulsen, P. M. E. 06 2005. Medisinske feil. Student project, Haukeland Sykehus. Available from http://www.helse-bergen.no.

[44] Vincent, C. January 2007. Incident reporting and patient safety. Editorial, British Medical Journal, Vol 334, p 51.

[45] Sari, A. B.-A., Sheldon, T. A., Cracknell, A., & Turnbull, A. January 2007. Sensitivity of routine system for reporting patient safety incidents in an nhs hospital: retrospective patient case note review. *British Medical Journal*, 334, 79–82. First published December 2006.

[46] Ben-Tovim, D. I. January 2007. Seeing the picture through "lean thinking". Letter, British Medical Journal, Vol 334, p 169.

[47] NRK. Story on medical treatment errors. "Puls", Norwegian television show on health issues. Available from http://www.nrk.no/puls, Jan 2007.

[48] Anderson, D. J. & Webster, C. 2001. A systems approach to the reduction of medication error on the hospital ward. *Journal of Advanced Nursing*, 35(1), 34–41.

[49] Nyssen, A. S., Aunac, S., Faymonville, M. E., & Lutte, I. 2004. Reporting systems in healthcare from a case-by-case experience to a general framework: an example in anaesthesia. *European Journal of Anaesthesiology*, 21, 757–765.

[50] Aase, K. Simulering som verktøy for å heve pasientsikkerheten. Lecture at Norwegian Air Ambulance conference 2007, Feb 2007.

[51] Vestby, T. 2005. Oppfatning av vern mht. uønsket innsyn i pasientjournaler. Survey by Kommunalansattes Fellesorganisasjon.

[52] Datatilsynet (The Norwegian Data Inspectorate). *Report from review, Helse Bergen, dept. Hagevik.*, June 2006. Available in norwegian only, from www.datatilsynet.no. Last viewed Oct. 30. 2007.

[53] Datatilsynet (The Norwegian Data Inspectorate). *Report from review of information security in patient journal system DocuLive and patient administration system PIMS at Helse Bergen HF, Haukeland University Hospital*, Aug 2006. Available in norwegian only, from www.datatilsynet.no. Last viewed Oct. 30. 2007.

[54] Datatilsynet (The Norwegian Data Inspectorate). *Report from review of confidentiality and availability of electronic patient journals at Akershus university Hospital HF*, Nov 2006. Available in norwegian only, from www.datatilsynet.no. Last viewed Oct. 30. 2007.

[55] Cappelen, I. & Lyshol, H. 2004. Oversikt over helseregistre i norge. *Norsk Epidemiologi*, 14, 33–38.

[56] Nystadnes, T. Bruk av standarder ved anskaffelse av helseinformatikksystemer. Kompetansesenter for IT i Helse- og Sosialsektoren, Mar 2007.

[57] Helse- Omsorgsdepartementet (Norwegian Department of Health). *Lov om helsepersonell m.v. (Norwegian law on health care professionals)*, 07 1999. Available from www.lovdata.no. Last viewed Oct. 30. 2007.

[58] Sosial- og helsedirektoratet (Directorate of Health and Social Affairs). *Code of conduct for information security in the health sector*, 2006. Available in Norwegian and English from www.shdir.no. Last viewed Oct. 30. 2007.

[59] Amoore, J. & Ingram, P. Aug 2002. Quality improvement report: Learning from adverse incidents involving medical devices. *British Medical Journal*, 235, 272–275.

[60] Marchette, D. 2001. *Computer Intrusion Detection and Network Monitoring - A statistical viewpoint*. Statistics for Engineering and Information Science. Springer Verlag, New York.

[61] Sikkerhetsråd, N. Mørketallsundersøkelsen 2006, 2006.

[62] EC. June 2006. Directive 2006/43/ec of the european parliament and of the council of 17 may 2006. *Official Journal of the European Union*, 157, 87–107.

[63] Gordon, L. A. & Loeb, M. P. Nov 2002. The economics of information security investment. *ACM Transactions on Information and System Security,*, 5(4), 438–457.

[64] Argyris, C. 1992. *On Organizational Learning*. Blackwell publishers, Cambridge, Mass.

[65] Hare, V. C. 1967. *System Analysis: A diagnostic approach*. Harcourt Brace & World, New York.