Introduction

Every incident indicates weaknesses in systems, networks, operations, incident preparedness and organisation that implies risk for new incidents. Learning from incidents is thus a great opportunity to improve the various parts of the information security system. When responding to incidents, there will always be some kind of learning present. When an organisation does nothing to react to or learn from an incident, the organisation learns that this kind of reaction is positive or negative dependent on the outcome of the reaction. Not learning from incidents implies continued risk for incidents in the future, thus organisations should seek productive learning, i.e. learning that yields improved security performance and restructures the values for security performance (Argyris and Schön, 1996). Productive learning from incidents and successful as well as unsuccessful responses to incidents will reduce the likelihood for occurrence of similar and dissimilar incidents in the future. Furthermore, productive learning will provide long-lasting preventing effects against a wide range of threats such as increased security awareness, organisational changes, improved technical systems and increased economical support for security.

Organisations can react to information security incidents in a lot of ways. One way is to ignore the incident, performing no incident response at all. Another approach is to
bring the system quickly back to normal, without achieving long-lasting learned
lessons. A different approach is to handle the deviation and learn in a manner that
provides long-term improvement of security. This paper is based on a hypothesis
stating that organisations react to incidents by short-term fixes without achieving
productive organisational learning. With this hypothesis as background, the paper
attempts to answer why organisations react to incidents without achieving productive organisational learning.

The paper concentrates on learning that goes beyond learning at individual level, and
explores organisational learning, i.e. learning that occurs when organisations acquire
information of any kind and by whatever means between people in the organisation
(Argyris and Schön, 1996). The concept organisational development is closely related
to learning (Levin and Klev, 2002), thus productive organisational learning from
incidents will develop organisations toward improved security performance.
Additionally, organisational learning will provide distribution of knowledge about
incident responding, thus creating redundancy of information among members. In
addition, learning from incidents at the organisational level can change the governing
values for security in the organisation, thus improving security. Hence, for long-term
security improvements from incidents, organisational learning should be encouraged.

In a general sense, learning from incidents is not a new concept (Cooke, 2003), there
are researchers who have looked at learning from safety incidents and major accidents,
e.g. Pidgeon (1997) and Lagadec (1997), and from incidents in sectors such as
banking (e.g. Stead and Smallman (1999)) and hospitals (e.g. Edmondson (1996)). In
the field of information security research, which traditionally have had a narrow
technical perspective (Dhillon & Backhouse, 2001), there has been written a lot about how to manage specific incidents and how to deal with specific technical problems (Hancock, 2001). Nevertheless, the learning process related to information security incidents has not been explored before. Hence, this paper provides new research within the field of information security.

By exploring barriers that prevent organisations to learn from information security incidents, the purpose of this paper is to answer why productive organisational learning from information security incidents is not achieved. The results from the study will provide a better understanding of obstacles to organisational learning from information security incidents, thus offering a possibility for improvement of learning from incidents.

The paper is divided into x sections. In the next section the theoretical framework for the empirical analysis is presented, including descriptions of incident learning, different orientations for learning in organisations and organisational learning. The theoretical framework ends by describing some barriers that may prevent incident learning.

**Incident learning**

What is incident learning? Let us first take a look at a definition of incident and then a look at the issue of learning. An incident can be defined as an unwanted and unexpected event representing a deviation from normal situation which may or may not result in loss. An information security incident is an incident that compromises

---

1 The sections empirical evidence and analysis + method and discussion/conclusion is not part of this version of the paper.
information’s confidentiality, integrity and/or availability. Learning involves something being altered by changed knowledge or behaviour (Levin and Klev, 2001). Learning may either be a product, something learned, or the process that creates such a product (Argyris and Schön, 1996). Hence, incident learning is the product or process that changes current knowledge or behaviour based on an unwanted and unexpected representing a deviation from normal situation.

Incident response is the process of handling a information security incident, typically handling a deviation (“putting the fire out”) minimizing e.g. downtime and loss of business and economical consequences. An incident will not necessarily announce its arrival, thus it is important to have an adequate response systems. There exists several guidelines for preparing incident response (e.g. Schulz et al, 1990 and West-Brown et al, 2003). These guidelines are directed at establishing and following written procedures for handling incidents, and focus in a less degree on the important learning process. The standard ISO-17799 follow the same thought as the guidelines; establish procedures for reporting of security incidents, security weaknesses and software malfunctions in order to set “out an action to be taken on receipt of an incident report” (ISO-17999). Follow-up and learning is seen as important parts of these guidelines. In order to improve and adjust the response systems to the organisation’s context, learning is important.
Cooke (2003) has suggested a general incident learning cycle, which is “a collection of organisational capabilities that enable the organisation to extract useful information from incidents of all kinds and to use this information to improve organisational performance over time”. This cycle is illustrated in Figure 1. It consists of several actions leading to learning which he argues set in motion respectively information sharing with others, incident recall and finally corrective actions. An incident learning cycle as the one shown in Figure 1 corresponds to what Argyris and Schön (1996) refer to as single-loop learning. Single-loop learning is learning that changes strategies of actions or the underlying assumptions for these strategies within the values of a theories of action, e.g. deviation handling. In contrast to single-loop learning, double-loop learning changes the values of theory-in-use, i.e. the theory of action that is implicit in the performance of the pattern of activity, thus creating new systems of value, as well as carrying out corrective actions like in the single-loop learning. In Figure 2 the relationship between single- and double loop learning is illustrated.
Responding to incidents always includes correction of deviation, since an important part of incident response is to bring the system back to normal as quickly as possible. Thus single-loop learning will happen for good or for bad during incident response. Productive double-loop learning should be encouraged during incident response, as this will change the underlying basic values for security in the whole organisation, creating increased security and decreased risk for incidents. Additionally, double-loop learning will improve the single-loop incident learning cycle by changing the basic values of the related theories-in-use.

**Learning in organisations**

The most effective learning from incidents happens at an organisational level, since this learning will provide distribution of knowledge among organisational members. Thus redundancy of information is created, i.e. overlapping of information about security activities among members. Organisational development is closely related to learning (Levin and Klev, 2002), so productive learning at an organisational level will support organisational development toward increased security performance. It can be claimed that there are four orientations of learning in organisations; cognitive learning at the individual level, learning through practical work, learning in artefacts and learning through social relations.
Cognitive learning at the individual level is an essential assumption for learning in organisations (Argyris and Schön, 1996), but it is not a sufficient assumption for a learning organisation (Levin and Klev, 2002). Individual learning do not necessarily imply organisational learning, as an organisation is a interplay between members of the organisation. Individual knowledge becomes organisational knowledge when individuals interact (Nonaka and Takeuchi, 1995). If the organisation shall benefit from the individual knowledge, individuals must think and act in a way that creates productive learning for the organisation, i.e. individuals must function as agents of organisational action (Argyris and Schön, 1996). The interaction between individuals and organisation implies that the arrow points in both directions; the learning of individuals who interact with one another is essential for learning at an organisational level, which feeds back to influence learning at the individual level.

Brown and Duguid (1991) on their side, describe how learning might happen in practical work, learning-in-working, as they look at learning in communities-of-practice. Learning happen through access to and membership of communities-of-practise, members do not gain explicit, formal “expert” knowledge, but the skill to behave as members of the community. Members acquire knowledge through social interactions with colleagues, e.g. through story-telling.

A third orientation, learning through artefacts shows how knowledge can be distributed to other organisational members by the help of knowledge embedded in artefacts. In an article about the building of the great Gothic cathedrals long before modern construction plans, techniques and calculation were available, Turnbull (1993) describes how an important part of the building of the cathedrals was distribution of
knowledge through artefacts. The artefacts used in the building were templates representing how stones should be cut in order to give a “stable, enduring and coherent structure, despite a discontinuous process and radical design and structural changes”. Several centuries after the first Gothic cathedrals were built, it is still possible to find similar distribution of knowledge by artefacts in the field of information security. The way insecure sources in open source operating systems, e.g. Linux, are fixed, have many similarities to the knowledge distribution in artefacts. The social processes of developing Linux-code is brilliantly described by Raymond (1998). Although Raymond has been criticized by Bezroukov (1999a; 1999b) for some weaknesses, e.g. being to simplistic, Raymond’s description provides a good illustration of the learning process in the open source development. The artefact is the open source, which is distributed among a community of interested people. The source is modified and commented among these people in a process creating an improved and more secure source.

A fourth type of learning is learning through social relations. The concept organisational learning is closely related to learning through social relations, since organisational learning is learning that takes place between people in an organisation. Among important contributors of theorizing organisational learning can Senge (1990), Nonaka and Takeuchi (1995) and Argyris and Schön (1996) be mentioned. Argyris and Schön (1996) say that organisations learn when it acquires information of any kind and by whatever means between people in the organisation. Organisational learning occur when members of an organisation learn between themselves on behalf of the organization or learning between groups and larger units of an organization.
As argued, the most effective learning from incidents happen at an organisational level. Organisational learning seem to be an appropriate theoretical framework for answering the research question in this paper, as organisational learning deal with learning between members, creating distribution of knowledge. Moreover it can be said that organisational learning implies that the organisation as a whole learns, thus the organisation as a unity will be better prepared for incidents in the future.

**Organisational learning**

The field of organisational learning has received increasingly attention from both academics, consultant and practitioners, which among other things is shown through a large number of publicised writings. Review articles such as e.g. Levitt and March (1988) give an idea of the variety of theoretical orientations. Senge (1990), Nonaka and Takeuchi (1995) and Argyris and Schön (1996) can be mentioned among the most popular and important contributions to organisational learning over the last years. In this paper I have chosen to use Argris and Schön (1996) as a theoretical foundation for answering the research question. There are mainly two reasons for this choice. First Argyris and Schön give a deep understanding of the learning process in organisations and why learning may not happen. Second, as shown in the next paragraph, their theoretical framework corresponds well to incident learning.

Experiencing surprising mismatches between plans or intensions and the actual outcomes, e.g. information security incidents, produce opportunities for organisational learning (Argyris and Schön, 1996). The experienced mismatches demand detection, thus detection systems as well as awareness among members are necessary for organisational learning from incidents. The mismatch constructs doubt which is
solved by organisational inquiry; thought and action that moves from doubt to the resolution of doubt, which changes organisational theory-in-use. In order to become organisational, the learning must become embedded in the images of organisation held in its members’ minds and/or epistemological artefacts (maps, memories and programs) embedded in the organisational environment. Argyris and Schön’s (1996) theoretical framework is well suited for incident learning. The inquiry due to surprising mismatches corresponds well with information security incidents. In addition single-loop learning corresponds to handling deviations quickly which is a natural part of incident responding, while double-loop illustrates the deeper learning related to the incident learning.

While Argyris and Schön (1996) have related organisational learning to inquiries associated to surprising mismatches between intention and actual outcome, Nonaka and Takeuchi (1995) focus on creating knowledge through a knowledge spiral triggered by planned events, as the identification and design of the problem is decided in advance. Engeström (19xx) has criticized Nonaka and Takeuchi for, among other things, this lack of questioning and analysing in the beginning of the knowledge spiral. He further criticizes Nonaka and Takeuchi’s knowledge spiral for being to static. These critiques indicate that Nonaka and Takeuchi’s framework is not suitable for incident learning, which occur in a dynamic environment with a demand for high-speed response.

Peter Senge’s (1990) ‘The Fifth Discipline’ has been a popular source about organisational learning, not least among practitioners. Senge (1990) can be described
as popular science, his framework is quite normative and do not provide the deeper understanding of organisational learning that we seek in this paper.

**Barriers against organisational incident learning**

There are several considerable obstacles for learning processes in incident responding (Lagadec, 1997). This section will, based on previous research, present some barriers against organisational learning and some barriers against incident learning picked from other fields than information security. Studies of organisational learning and incident learning show that there is a variety of different learning barriers at both organisational and individual levels.

As argued in the previous section, I have claimed that organisational learning as presented by Argyris and Schön (1996) provides a good framework for understanding organisational learning from incidents. Our journey through different barriers thus starts with Argyris and Schön’s (1996) suggested obstacles. According to Argyris and Schön there are some conditions that reduce the likelihood that individuals will engage in organisational inquiry that leads to productive learning. When individuals deal with issues that are threatening or embarrassing, their reasoning and action match a particular model of theory-in-use (Model I) which enter into primary inhibitory loops that can be explained at three levels; individual, organisational and an interaction of the two. In situations that feel embarrassing or threatening, individuals will seek to remain control of the situation and acts accordingly (Argyris, 1990). Generally speaking, individuals develop a set of defence mechanisms that prevent them from threatening or embarrassing situations. In addition, mechanisms to hide the
defence mechanisms are created, e.g. individuals do know that they are acting wrong but create ways to make it look like they have not done mistakes (Argyris, 1990).

At an organisational level secondary inhibitory loops inhibit productive learning. Secondary inhibitory loops includes among others, organisational defensive actions and policies that protect individuals from experiencing embarrassment or threat, while at the same time preventing individuals or the organisation as a whole from identifying the causes of the embarrassment or threat in order to correct the relevant problems. Argyris (1990) argues that organisational defences make it likely that individuals, groups, interest groups and organisations will not detect and fix errors that are embarrassing or threatening because the basic rules are to (1) bypass errors and pretend not to, (2) make the bypass impossible to discuss and (3) make sure that it is not possible to discuss the impossibility to discuss the bypass.

The result of these individual and organisational defences described by Argyris and Schön (1996) and Argyris (1990) are reduced likelihood for organisational learning around issues that are embarrassing or threatening. Within the field of information security, situations might feel embarrassing or threatening since incidents can imply legal offences, might harm an organisation’s reputation and some mistakes (e.g., downloading virus infected games at your office computer) might be hard to admit.

The defensive patterns derived when dealing with embarrassing or threatening issues not only undermine single-loop learning, they inhibit double-loop learning as well. This problem is shown in what Argyris and Schön (1996) denotes the learning
paradox, Argyris and Schön argue that actions taken to promote productive organisational learning actually inhibit deeper learning.

Organisational characteristics and the organisational culture influence incident learning, there are many context dependent organisational characteristics that influence the ability to learn from incidents. Edmondson (1996), who discusses how groups have barriers against admitting and learning from mistakes in hospitals, shows some organisational characteristics influencing the willingness to learn from incidents; the behaviour of nurse managers, how past incidents have been handled and how conclusions from former incidents have been drawn. These conditions are further strengthened through conversations between organisational members. In this way, perceptions of the consequences of making mistakes are created, which creates a climate influencing the ability to learn. The working environment thus plays a vital role for the possibility to learn from incidents.

The security culture will affect the learning in a positive or negative way depending on the quality of the security culture. In a study of lessons learned from three major incidents from the banking industry, Stead and Smallman (1999) argue that an organisational culture can prevent learning from incidents. Such an organisational culture can be characterized by factors such as management commitment, staff non-disclosure agreement, naïve assumption (e.g. ‘this simply didn’t happen to us’), shortcomings of monitoring and lack of information exchange. Pidgeon (1997) sees organisational learning as a part of an safety and reliability culture, which I claim is equal for security culture since security just like safety and reliability is related to
protection of assets. He further argues that the culture might influence learning in a bad or good way, dependent on the quality of the culture.

Political dilemmas in an organisation reduce the likelihood for incident learning (Pidgeon, 1997; Cooke, 2003). Pidgeon (1997) points at political barriers against learning such as; conflicts over narrow-minded interests leading to faulty reporting of incidents, secrecy, normalisation of errors in the face of external accountability and the reinterpretation of failure as success. At the heart of this issue is the dilemma of blame. Cooke (2003) adds the issue of legal offences as an important part of the political dilemmas. The issues of blame and legal offences increases the possibility of interpreting learning situations as threatening or embarrassing, which are major obstacles to learning according to Argyris and Schön (1996).

Understanding the issue of power is essential in order to explore the political dilemmas that might prevent incident learning. I have already described that organisational learning and organisational development are closely related, according to Levin and Klev (2002) organisational development is not possible without involving power, accumulating power and changing power relations. Which individuals and groups that have access to decision arenas related to incident response and incident learning will influence the outcome of learning. Asymmetries in power relations in social settings may make some standpoints preferable to other standpoints, although those in less powerful positions may see matters most clearly (Pidgeon, 1997). By playing the political game in their favour, a group within the organisation might e.g. prevent productive learning in order to defend their position in the organisation. There are a lot of different sources to power, which all can be obstacles
as well as an initiators for productive learning. Overviews of sources to power are described by e.g. Morgan (1986) and Bolman and Deal (1998). In relation to incident learning, one source seem to be especially interesting. The old saying “knowledge is power”, is legitimate in understanding power relations in the field of information security. Lack of skills and knowledge might reduce the likelihood for inquiry when dealing with mismatches. When dealing with a mismatch, individuals may not know how to deal with the incident or they may not even know that there is a security incident. Hence, those with the necessary skills and knowledge sit in a position with a lot of power that can influence the learning outcome.

Until now obstacles related to the organisational learning process have been described, we will now turn the attention to barriers related to incident learning. The following barriers will mainly be related to single-loop learning. Cooke (2003) argues that learning from incidents do not take place because organisations lack an effective incident learning system. In the following I will look at obstacles related to some of the different steps in the single-loop cycle presented in Figure 1, starting with identification and reporting.

Detecting the incident is certainly necessary if response and learning shall take place. Having an inadequate threshold for detection may be an obstacle for inquiry (Cooke, 2003), thus preventing productive learning. For example may the possible severity of the incident influence the likelihood for detection.

Reporting and communicating incidents are important factors for incident learning between individuals. Hence, whistleblowers, e.g. the employees who stood up
blowing their whistles and telling about what went wrong in the economical scandals at Enron and WorldCom, are important contributors for productive learning. The willingness to report and talk about incidents is closely related to political dilemmas as well as if the situation is embarrassing or threatening. Within the field of industrial safety, Kjellén (2000) points out several contributions for not reporting incidents and accidents; severity of incident/accident, being afraid of being judged as careless or accident-prone, size of the company, period of employment, insufficient incentives that promote reporting, disadvantages of reporting, advantages of not reporting, negative consequences to the individual if reported/not reported. In a study of incident learning in hospitals, Edmondson (1996) shows that the more errors are reported and discussed, the more willing organisation members are to report errors in the future. This is strongly related to how safe members interpret it is to discuss mistakes they have done, e.g. how members believe that making a mistake will not be held against them.

The next two steps in Cooke’s (2003) learning cycle is the investigation and causal structure. Perrow (1999) says that learning might become erroneous, when organisations do not find the right causes of the incident and thus takes the wrong countermeasures. This problem correlates to what Argyris and Schön (1996) refers to as “superstitious learning”, lessons learned that are based on the belief that because events have followed one another in time they are also related to one another as cause to effect. Hence, learning might be based on erroneous lessons, thus not resulting in productive learning. Another problem for productive organisational learning is that members learn, but learn the wrong things (Perrow, 1999); “they learn that disasters are rare and they are not likely to be vulnerable so, in view of the attractions of
creating and running risky systems the benefits truly do outweigh the risks for individual calculators”.

Cooke (2003) draw attention to learning between organisations as a part of the learning cycle. Organisations are recommended to report information security incidents to national organisations such as the Centre for Information Security (SIS) in Norway and the CERT Coordination Centre (CERT/CC) in the US. These organisations are assigned to collect incidents and tell other organisations about the incidents, thus providing a great potential for other organisations to learn about incident handling and potential incidents. If such an arrangement shall work as intended, it is demanded that organisations report their incidents. As I have already described information security incidents might be embarrassing or threatening to individuals and organisations, thus preventing reporting of incidents to the outside of the organisation. Especially since incidents might destroy the organisation’s reputation, which might e.g. lead to loss of customers. Hence, reporting to organisations such as SIS and CERT/CC might increase the likelihood that organisations try to ignore or hide incidents, thus preventing productive learning. The only learning apparent will be learning to keep away from trouble. Another pitfall might be that such reporting results in a belief that “if we report, someone else will take care of the learning”. In a case study of three major incidents in the banking industry, Stead and Smallman (1999) argue that organisations in the same sector do not make contact with an organisation that suffers a disaster. Hence, as Lagadec (1997) puts it; learning across organisations become even more problematic than the learning within an organisation.
The corrective actions finalizes Cooke’s (2003) learning cycle. The resulting action might be effective for information security, but need not to be effective or efficient for other parts of the organisation. Dependent on how important information security is looked at compared to other business processes, this dilemma may prevent productive learning. According to Argyris and Schön (1996), the value of an action depends on how the question ‘effectiveness or efficiency for what?’ is answered. Economical aspects may prevent productive learning, as described by Rasmussen (1997). He describes how pressures towards economic efficiency and least possible work increase risk.

The incident learning cycle can in itself become an obstacle to learning. Based on former success, organisations might find a single-loop pattern to handle deviations. Argyris and Schön (1996) refer to this problem as “competence traps”. The organisation becomes trapped with an inherent pattern, which is not the best learning cycle the organisation can have. As the organisation stick with one given solution for problem solving, the most appropriate incident response system is not present.

There are many different barriers at individual and organisational level that prevent productive organisational learning from incidents. Some of these barriers have been presented above as a theoretical foundation for the rest of the present study. Based on the theoretical framework in this section the present study attempts to answer why productive organisational learning is prevented at organisational and individual level and further why respectively double-loop and single-loop learning is prevented.
References


Bezroukov, N. Open Source Software Development as a Special Type of Academic Research (Critique of Vulgar Raymondism). First Monday, 1999a, vol. 4, no. 10. Available at: [http://firstmonday.org/issues/issue4_10/bezroukov/index.html]


Engeström, Y. Innovating learning in work teams: analyzing cycles of knowledge creation in practise, [unknown source]


ISO 17799: Information Security Management


Senge, P.M. *Den femte disiplin*. Hjemmets bokforlag, 1990. [in Norwegian]

