Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2007 Proceedings

European Conference on Information Systems (ECIS)

2007

Organizational Learning for the Incident Management Process: Lessons from High Reliability Organizations

Wilem J. Muhren
University of Tilburg, w.j.muhren@uvt.nl

Gerd Van Den Eede
gerdvde@gmail.com

Bartel Van de Walle
University of Tilburg, bartel@uvt.nl

ORGANIZATIONAL LEARNING FOR THE INCIDENT MANAGEMENT PROCESS: LESSONS FROM HIGH RELIABILITY ORGANIZATIONS

Muhren, Willem, Tilburg University, Warandelaan 2, 5000 LE Tilburg, The Netherlands, w.j.muhren@uvt.nl

Van Den Eede, Gerd, Vlekho Business School, Koningsstraat 336, 1030 Brussels, Belgium, gerd.vandeneede@vlekho.wenk.be

Van de Walle, Bartel, Tilburg University, Warandelaan 2, 5000 LE Tilburg, The Netherlands, bartel@uvt.nl

Abstract

Mainstream organizations typically struggle in their quest to combine effectiveness with efficiency, or reliability with flexibility. Experimentation and trial-and-error are regarded as important processes for organizational learning, but do not always lead to an organizational-wide optimum in terms of efficiency. Certain organizations, so-called High Reliability Organizations (HROs), exist that operate in hazardous environments but manage to structure themselves to be efficient and stay highly reliable. These organizations in high-tension industries are deprived from the luxury of going through trial-and-error learning, but we state that exactly this is accountable for the HROs' success. Through a case study of the IT Incident Management process at a large European financial services provider, we investigate how people involved in a process of such a mainstream organization, where reliability is of great concern, can learn from HROs to achieve a greater reliability while working efficiently. It appears that the characteristics that make an HRO distinct from other organizations are – at least to some extent – present in the IT Incident Management process. Our main conclusion however is that considerable opportunities remain unseized to lift the HRO qualities to a still higher level.

Keywords: Incident Management process, Organizational learning, High Reliability Organizations.

1 INTRODUCTION

Today's organizations are characterized by 'raplex' – rapidly evolving and complex – contexts in terms of technology, competition, legal and institutional obligations (Nooteboom, 1998). Only those organizations survive and prosper that are capable of dealing with these raplex conditions. Organizations need to be flexible in order to respond to raplex conditions swiftly or, even better, anticipating them (Hong et al., 2004). In organization theory, this paradigm is known as 'Organizational Learning'. An organization that demonstrates organizational learning in a durable and semi-continuous way is known as a 'Learning Organization' (LO).

From an efficiency perspective, it can be said that an organization's components have to be tightly coupled (Wolf, 2001). Indeed, when the processes between individuals, subunits, ideas, procedures, hierarchical levels (Orton & Weick, 1990) are integrated as far and smoothly as possible, costs will be the lowest, time will be saved and the least energy and resources will be wasted. Through organizational learning's highly praised processes of trial-and-error (Aase & Nybø, 2005), the aforementioned organizational components learn which activities yield the highest performance for themselves and the organization as a whole.

Paradoxically, because of the difficulty to realize the necessary mutual adjustments, organization members notice that the probability of achieving the ideal situation of tight-coupling on an organization-wide level is too low to be worth striving for. Moreover, they realize that such a strategy would go at the expense of their own component's efficiency. For this reason, actions are often adjusted in view of a sublevel's optimum (Denrell). The result is a sub-organizational optimum and an organizational suboptimum, the overall result being a loosely coupled and not optimally efficient organization.

High Reliability Organizations (HROs) are organizations that have histories of very safe operations although they operate in environments where accidents could have an enormous impact (Roberts & Libuser, 1993), like aircraft carriers (e.g. Rochlin et al., 1987) and organizations in the nuclear industry (e.g. Roberts, 1990). HROs are exhibiting a rare combination of reliability and flexibility, of effectiveness and efficiency (Van Den Eede et al., 2004).

We argue that because of the absence of 'trial'-and-error learning in these high hazard environments, the actors in HROs will not 'learn' that it is wiser to pursue their own optimum. Instead, they will continue to pursue the image of a tightly-coupled organization. The result thereof is efficiency. As such, we state that the fact of being deprived from the luxury to go through a lot of trial-and-error learning is accountable for the HROs' success. However, as we have mentioned above, organizations do not only need to be efficient, they need to be reliable as well. This calls for a balancing act between tighter and looser coupling. As we will see, HROs exhibit five different antidotes for tight-coupling. The result is an organization that combines the best of tight-coupling with the best of loose-coupling.

In this contribution we want to investigate how an organization operating in raplex conditions can learn from HROs in being both efficient and reliable, despite the fact of an absence of organizational learning's characteristic trial-and-error processes.

In the subsequent section we will describe HROs and their characteristics that make them highly reliable while staying efficient. Next, we will present a case study of the IT Incident Management process at a large financial institution. Through an ethnographic study we examined how they can learn from HROs to balance both virtues of reliability/effectiveness and flexibility/efficiency.

2 HIGH RELIABILITY ORGANIZATIONS

2.1 Introduction

An organization is exposed to all kinds of threats from various internal and external sources. The organization may protect itself from these threats, but threats can still cause an organizational accident, as depicted in Figure 1.

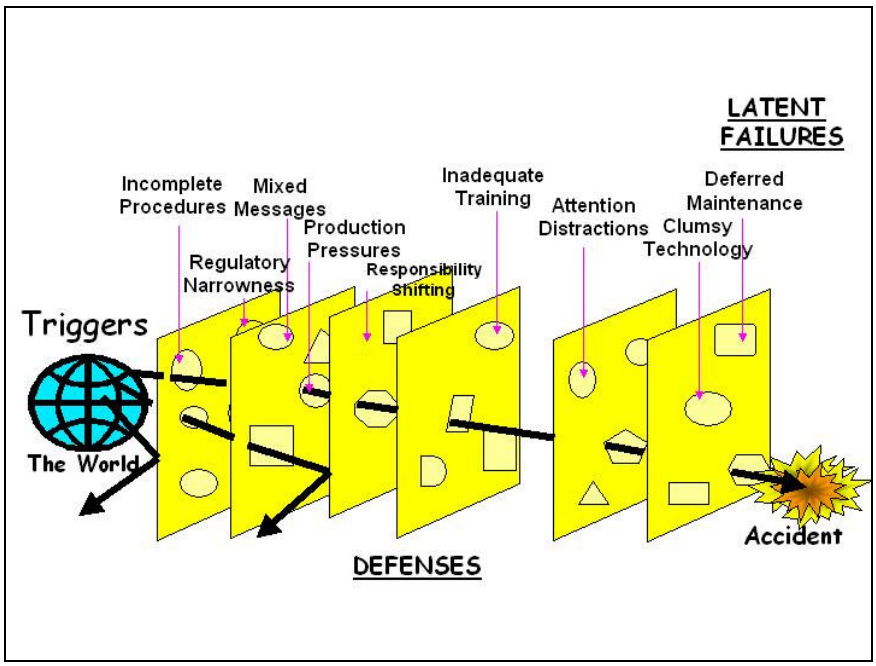

Figure 1. Swiss Cheese Model (Reason, 1997)

James Reason's Swiss Cheese Model (1997) is a metaphor stating that an organization's barriers of defense can be thought of as the slices of a Swiss Cheese. Each defense is not always functioning optimally and may contain holes, which are at different 'locations' in the different slices. In addition, when one hole is plugged, another one may emerge elsewhere. If at one point in time, all holes happen to line-up, a latent danger becomes manifest as it bypasses all built-in defense mechanisms causing an organizational accident.

Organizations operating under high-risk circumstances are very vigilant on avoiding accidents, because their occurrence would have disastrous consequences, either for the organization itself or for the public. Despite the fact that they operate under trying conditions, they have less than their fair share of accidents (Weick & Sutcliffe, 2001 p 9). Such organizations are labeled "High Reliability Organizations" (HROs) and can be identified "by asking the question: *'How often could this organization have failed with dramatic consequences?'*. If the answer to the question is many thousands of times, the organization is highly reliable." (Roberts, 1990)

Processes in HROs are distinctive because they focus on failure rather than success, inertia as well as change, tactics rather than strategy, the present moment rather than the future, and resilience as well as anticipation (Weick et al., 1999).

Early characterizations of HROs emphasized the total elimination of error, while later on researchers concluded that errors are inevitable and HROs are not error-free, but that errors do not disable them (Weick, 1987; Weick & Sutcliffe, 2001 p 14). Effective HROs are known by their capability to contain and recover from the errors they make and by their capability to have foresight into errors they might make. Reliability is the number one concern for HROs (Weick et al., 1999; Roberts, 1990).

2.2 Characteristics of High Reliability Organizations

HROs are so reliable because they have a certain state of 'mindfulness' (Weick & Sutcliffe, 2001 p 42). According to Weick et al. (1999), mindfulness is less about decision-making, which is the traditional focus of organizational theory and accident prevention, and more about inquiry and interpretation grounded in capabilities for action. HROs possess five key qualities to reach their state of mindfulness (Weick et al., 1999), represented in Figure 2. These qualities enable HROs to compensate for their inherent tight-coupling with attributes that loosen their coupling, hence contributing to a balance between efficiency and reliability. Through their preoccupation with failure, reluctance to accept simplifications, and sensitivity to operations, HROs are able to anticipate and become aware of dangers. HROs are able to contain dangers when they are spotted because they are sensitive to their operations, committed to resilience and deferred to expertise.

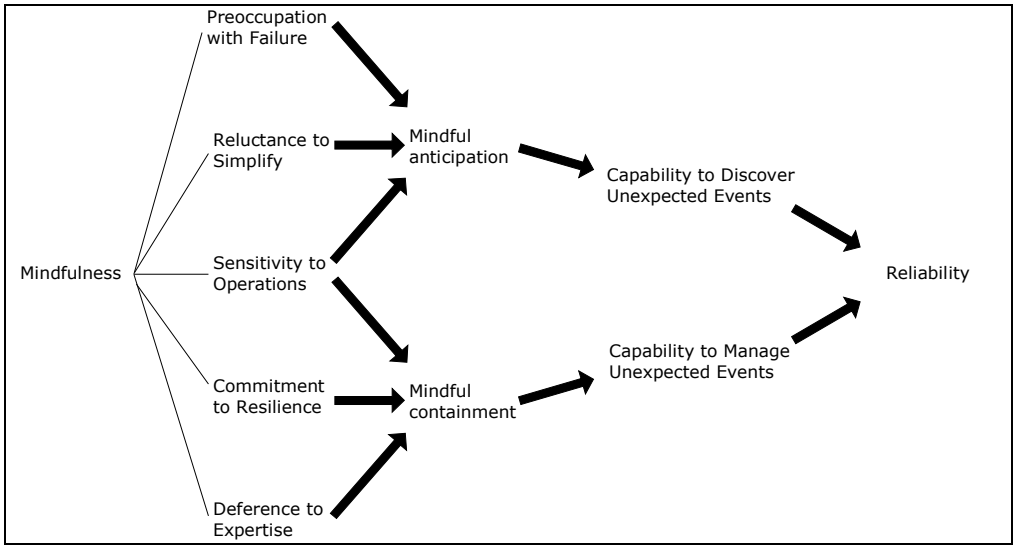

Figure 2. A Mindful Infrastructure for High Reliability (adapted from Weick et al., 1999)

In the remainder of this section, we outline the different HRO principles that make up the mindfulness of an HRO, drawing heavily from the extensive body of research by Weick and co-workers (Weick et al., 1999; Weick & Sutcliffe, 2001).

Preoccupation with failure

Preoccupation with failure is an important principle that gives HROs a distinctive quality, for HROs are preoccupied with something they seldom see. Although HROs are successful in avoiding incidents, they do not boast about their superiority. HROs are wary for the common failures after success, caused by restricted search, reduced attention, inertia, risk aversion, and homogeneity. They treat even the smallest error as a sign that something could be wrong with the system, i.e. with one of the defense layers, and they are anxious that the holes in the cheese might line up. HROs regard close calls as a kind of failure that reveals danger, and not, as most other organizations would do, as evidence of success and their ability to avoid accidents. Members of HROs know that they cannot foresee everything: They know that they do not know, and they expect to be surprised. That is why members of HROs are constantly worried that they make analytical errors and that these errors might be amplified, in combination with limitations to foresight, and lead to accidents.

Reluctance to simplify

HROs take deliberate steps to create more complete and differentiated pictures of what is going on. Because HROs believe that the world they face is complex, unstable, unknowable, and unpredictable, they try to notice as much as possible. Simplifications produce blind spots, so HROs differentiate in

order to get a more varied picture of potential consequences and in turn a richer and more varied set of precautions and early warning signals.

HROs make fewer assumptions, cultivate requisite variety and socialize people to notice more. The law of requisite variety was originally proposed by Ashby (1958), and suggests that the larger the variety of actions available to a system, the larger the variety of perturbations in its environment it can compensate. HROs stimulate frequent job rotation and hire employees with non-typical prior experience. By these means HROs obtain a broader divergence of perspectives, which leads to a broader set of assumptions that sensitize it to a greater variety of inputs. Diverse groups have more information available than more homogeneous groups, but communication patterns and cognitive limitations often lead to a situation where unique information does not get shared. Unique knowledge must be surfaced. Rutkowski et al. (2006) studied the use of a group decision support system (GDSS) to identify unique but hidden knowledge that resides in a group. This unique knowledge appeared to be of key importance and would not have been shared without the use of the GDSS.

Sensitivity to operations

HROs try to signal errors when they are still tractable and can still be isolated by attaining well-developed situational awareness. Situational awareness is defined by Endsley (1997) as "the perception of the elements in the environment within a volume of time and space; the comprehension of their meaning and the projection of their status in the near future". Sensitivity to operations is about the overview of the 'Swiss Cheese' and constantly trying to find out where the holes are located in the cheese. HROs consistently communicate the big picture of what the organization seeks to do, and try to get everyone to communicate with each other about how they fit in the big picture (Roberts & Bea, 2001). With a situational awareness and a big picture, people in HROs can make continuous adjustments that prevent errors from accumulating and enlarging.

Sensitivity to operations is achieved through a combination of shared mental representations, collective story building, situation assessing with continual updates, knowledge of physical interconnections and parameters of the organization's systems, and active diagnosis of the limitations of preplanned procedures.

Commitment to resilience

Resilience is a combination of keeping errors small and improvising workarounds to keep the system functioning. People in HROs are so committed to resilience, that they see this 'firefighting' as evidence that they are able to contain the unexpected. In contrary, managers in business may perceive successful firefighting as evidence that they are distracted and therefore unable to do their normal work (Weick & Sutcliffe, 2001 p 70).

HROs need to have a broad repertoire of actions they can make use of when a danger occurs. HROs support improvisation to be able to recombine the actions in their repertoire into novel combinations. As Wildavsky (1988 p 70) describes, "improvement in overall capability, i.e. a generalized capacity to investigate, to learn, and to act, without knowing in advance what one will be called to act upon, is a vital protection against unexpected hazards". Informal networks are a common resource for HROs to respond to dangers resiliently, because they provide an infrastructure that is needed to handle unanticipated dangers in a swiftly manner. When events get outside of normal operational boundaries, knowledgeable people organize themselves into ad hoc networks to provide expert problem solving.

Deference to expertise

What people in HROs have mastered is the ability to alter typical hierarchical patterns of deference when the tempo of operations changes and unexpected problems arise. Decisions are then made on the front line by people who have the most expertise, regardless of their rank. In these situations, expertise and experience are usually more important than rank, so the decision structure in HROs is a hybrid of hierarchy and specialization. This shift to anarchy comes from a collective, cultural belief that the necessary capabilities lie somewhere in the system and that migrating problems will find them.

3 CASE STUDY: THE INCIDENT MANAGEMENT PROCESS

3.1 Introduction

Financial institutions are supposed above all other virtues to be trustworthy (Heller & Willatt, 1977 p 11). The fundamental commodity in which financial institutions deal is not money but confidence, and a loss of confidence, unlike loss of money, cannot be dealt with simply by a write-off in the balance sheet (Heller & Willatt, 1977 p 16). In other words, a financial institution must be reliable.

In this section, we report on an extensive research program we conducted of the IT Incident Management process at a large European financial services provider active in the fields of banking and insurance. The objective of our research was to investigate how the people involved in the Incident Management process can learn from HROs to achieve a greater reliability. The financial institution has branches all over the world and offers its services to millions of clients, individual clients as well as retail clients and multinational companies. The financial institution holds a Euro zone top 20 ranking in terms of market capitalization. The financial institution's IT department employs about 2,000 people.

The Incident Management process is part of a larger framework for best practices in IT service management, the Information Technology Infrastructure Library (ITIL). The primary goal of the Incident Management process is to restore normal service operations as quickly as possible and to minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. An incident is defined as "any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service" (Central Computer & Telecommunications Agency, 2000 p 71). This can vary from smaller incidents (e.g. a printer that does not work) to incidents with a higher impact (e.g. a mainframe failure).

3.2 Organization of the Incident Management process

Figure 3 shows the organization of the Incident Management process at the financial institution.

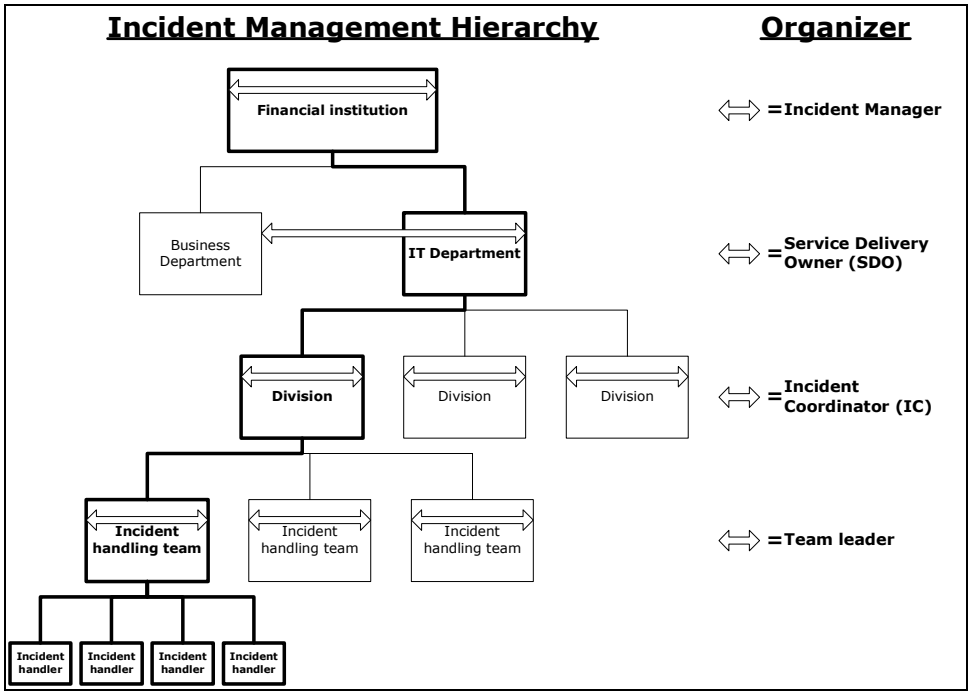

Figure 3. Organization of the Incident Management process

Coordination across the IT department

The financial institution has a special Service Management division that coordinates the ITIL processes throughout the organization. One of the Service Management division's staff members is the Incident Management process owner, in ITIL referred to as the Incident Manager. The Incident Manager is responsible for the efficiency and effectiveness of the Incident Management process. The Incident Manager monitors the Incident Management process, maintains the Incident Management application, and makes recommendations for improvement. The financial institution uses a special IT Service Management application suite, Peregrine Systems' ServiceCenter, which is designed to support ITIL's best practices.

Organization within service domains

The financial institution offers many services to their customers, e.g. asset management activities, financial transactions, and online banking. To support all these services, many internal services have to be in place. The financial institution has split up all her activities into service domains, and each of the over 70 service domains maintains one internal or external service. Every service domain has a Service Delivery Owner (SDO), who is responsible for supporting the service domain by the IT department. The SDO has a good overview of all activities within a service domain, from the IT department to the users in the business divisions, and is therefore an important contact person when incidents occur in a service domain. In literature on organization theory this role is known as 'boundary spanner' as it enables transgressing the departmental boundaries (Williams, 2002).

Organization within divisions of the IT department

Each division has its own Incident Coordinator (IC), who is responsible for the Incident Management activities within his division. The IC coordinates the Incident Management activities of the teams in his division and communicates with the SDO when a higher priority incident occurs. ICs provide the Incident Manager of recommendations for improvement of the Incident Management process.

Organization within incident teams

Each incident handling team has a team leader who is the contact person for the team.

3.3 Incident handling process

Once an incident is detected, it goes trough different steps before it can be closed.

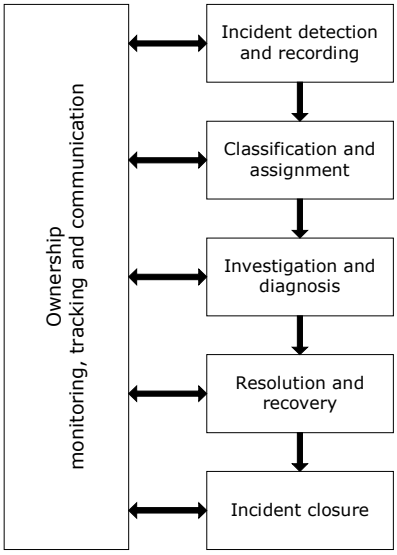

Figure 4. The Incident life cycle
(adapted from Central Computer & Telecommunications Agency, 2000)

It is important to note that an incident is constantly monitored by the owner of an incident, who makes sure the agreed resolution time is not exceeded and who communicates the status of the incident to the user.

The incident life cycle as shown in Figure 4 consists of incident detection and recording, classification and assignment, investigation and diagnosis, resolution and recovery, and finally incident closure. We will shortly describe these different steps next.

Incident detection and recording

When a user encounters difficulties in continuing her work, she calls the Service Desk, the first-line support for incident handling in the organization. It is an easy to memorize number, **505, because it visually resembles the word "SOS". If the difficulty cannot be solved immediately, the Service Desk registers it as an incident. An incident ticket is then created in Peregrine and all possible incident details are entered in the ticket. From this point onwards, the Service Desk is the owner of the incident and is responsible for the timely handling of the incident and the communication to the user. The user needs to be updated regularly on the status of the incident. An incident can also be detected by operational personnel. Operational personnel could either be the cause of the incident, or they were just able to detect the incident in their day-to-day activities before a user noticed any service disruption. In this case it is a common procedure that they register the incident in Peregrine. They will then be the owner of the incident and coordinate the incident until it is solved. In the remainder of this research we will focus on the normal procedure that the Service Desk coordinates incidents.

Classification and assignment

By asking targeted questions, the Call Desk can estimate the priority of the incident. The priority is set by determining the impact and urgency of the incident. The impact of the incident must be determined from the company's perspective and indicates the (potential) financial loss the incident can cause.

It is possible that the Service Desk is able to handle the incident, but cannot do this immediately. The incident is then assigned to the Service Desk. In most cases the Service Desk does not know what is causing the incident or how to solve it, so they must make an appeal to people with more expertise: second-line support groups, having more specialist skills, time or other resources to solve incidents. Because the Service Desk inquired the user about the incident, they will have an idea on what could be causing the incident or at least in what area to start investigating it. In Peregrine a list of teams appears that could be consulted for this kind of incident. The Service Desk assigns the most suitable team – in their view – to handle the incident.

People from the IT department are split up into teams that each has their own specialization. These are virtual teams, because they could comprise people who work in different divisions and/or at different locations. They all have access to Peregrine, and when an incident is assigned to a team, it appears in the mailbox of the specific team and each team member can assign the incident to himself or herself. The team member that assigns the incident to himself/herself is called the incident handler. When the incident appears is assigned to the wrong team, it is sent back to the sender.

Investigation and diagnosis

The incident handler will investigate the incident and try to find a solution or a workaround. It is possible that a solution can only be implemented after some time, e.g. at a new release. A workaround could be suggested that will help the user until the real solution is implemented. When a team member cannot identify the underlying cause of the incident and propose a solution or workaround to it, the incident can be further rerouted to a higher-line support group, even an external vendor, until a solution to the incident is found.

Resolution and recovery

The incident handler implements the solution or the workaround, takes all necessary recovery actions and updates the documentation of the incident in Peregrine by describing how she solved the incident.

Incident closure

The Service Desk contacts the user to make sure the proposed solution is satisfactory. If this is not the case, the incident is sent back to the incident handler. The Service Desk closes the incident when the user is satisfied with the proposed solution.

Incident briefing

Every morning the most important incidents that occurred the day before or the incidents that are still in the process of being handled are discussed. Employees who solved the incident or who know more about it, explain the cause of the incident and the (proposed) solution to a public comprising general managers, incident process coordinators, service delivery owners, and other IT staff that is involved in Incident Management or just is interested. The briefing can be attended 'live' at the head office of the financial institution or at another office via videoconference. Incidents are thoroughly analyzed and measures are taken to prevent the same kind of incident in the future.

4 OBSERVATIONS

For this work we applied a qualitative research approach using ethnography (Agar 1986; Hammersley & Atkinson, 1995; Myers 1999). We performed more than 800 hours of observations at the financial institution to obtain a clear picture of how the financial institution handles IT-related incidents. In this time frame we followed all the important actors of the Incident Management process, who are depicted in figure 3, in their daily work: the incident manager, the service delivery owners, the incident coordinators, the team leaders and some of the incident handlers. The hours at the financial institution were mainly spent on observation, general discussions with the people about their work, attending incident briefings and Incident Management process evaluation meetings, studying the previous Incident Management data from the Peregrine application and studying internal reports. Data analysis was conducted by interpreting the transcripts of our observations. Through this active observation, we were able to examine the mindful infrastructure that is in place at the Incident Management process.

We will give an overview of the HRO characteristics of the Incident Management process according to the five HRO principles that make up the mindful infrastructure as shown in figure 2.

Preoccupation with failure

There is a good infrastructure in place to report incidents, and employees use it frequently. We have noticed that, even when a small error occurs, people jump in to intervene and offer their assistance. A good example of their preoccupation with failure is the establishment of the incident briefing. However, not everybody in the organization is aware of the importance of learning from incidents through such a briefing. Only the highest priority incidents are discussed at the incident briefing. Some employees apparently do not feel like justifying their way of handling incidents, and so label and incident with a lower than actual priority in order to avoid having to appear at the incident briefings.

There are procedures in place how to handle certain incidents. But because of time pressure, procedures are not always updated after handling a new kind of incident, or are not entered in detail. A second-line incident handler expressed us his concern about such incomplete information in procedures: *"I easily loose ten to fifteen minutes when I am dealing with incomplete information. But what if for one reason or another that slack time would not be available?"* This employee was very concerned that he might face surprises that lead to failures, but apparently not everybody in the organization is that preoccupied.

Reluctance to simplify

The financial institution stimulates diversity in their staff by hiring people with non-typical experience for their job. For example, at one specific division of the IT department from where we were doing our research, out of about twelve staff members there were not even two people with the same background education. Moreover, the financial institution stimulates job rotation, which also contributes to the

requisite variety in their staff. Because the people are so divergent, the situations they face can be viewed from many different perspectives. This creates skepticism, leading to an instructive climate when people interact with one another and a qualitatively better assessment of the situation.

To oversee the complexity of the processes involved, the financial institution appointed Service Delivery Owners. Service Delivery Owners are the "boundary spanners" (Weick & Sutcliffe, 2001 p 11) who enable a successful end-to-end service throughout the organization.

However, at some points the financial institution does simplify. Key Performance Indicators, frequently applied by mainstream organizations (Van Den Eede et al., 2006), are used to measure the performance of different incident solving teams in a standardized manner. Mainly by paying attention to these evaluation criteria, incident handlers could loose their focus on other aspects of their work.

Sensitivity to operations

Several means are used to develop a strong situational awareness at the financial institution. There is a good intranet in place, where the latest developments are communicated and exhaustive information is available about the day-to-day activities of all divisions and teams. There are various internal magazines and news bulletins that communicate the big picture of the organization. Monthly an internal news report is shown in the theatre of the financial institution, every episode showing a.o. a different employee who is followed on a normal working day. There are monthly briefings by the Chief Information Officer to communicate the future plans of the IT department and to give an opportunity for discussion and feedback. The financial institution's external strategies are also elucidated by means of these media. There was for example an advertising campaign on national television, and the purpose of this campaign was explained on the intranet.

Commitment to resilience

The incident handlers we have interviewed were all very committed to their work in resiliently responding to incidents. They spoke about their work with passion and regarded themselves irreplaceable in their 'firefighting'. The financial institution shows their commitment to resilience in the incident briefings discussed previously. There is a good resilient infrastructure in place by informal networks. People have their connections throughout the organization and therefore perfectly know whom to contact when a critical situation arises.

However, there is not much time for training in handling incidents. As a senior executive stated, "this is a waist of time, because there are many incidents in real-life that incident handlers can learn from".

Deference to expertise

Incident handlers at the financial institution make up the front-line for responding to incidents. When an incident occurs, there sometimes is hardly any time to ask superiors for permission to take important decisions. Incident handlers are allowed to make these important decisions when the necessity emerges and there are no procedures to handle them. Later on, incident handlers must justify their actions, but there will be no penalty for bypassing their superiors. It is remarkable that this is not documented anywhere, but all incident handlers agreed that this was a common practice.

5 DISCUSSION

All HRO characteristics are – at least to some extent – present in the Incident Management process. However, the findings from the case study show that there are also indications of less mindful and non-HRO like behavior. HROs have different mechanisms at their disposal to improve the level of mindfulness. Therefore, our main conclusion is that considerable opportunities remain unseized to lift the HRO qualities to a still higher level. In this respect we advise the financial institution to improve their level of mindfulness. As Roberts and Bea (2001) state, HROs invest disproportionately more money in training people to recognize and respond to anomalies than other organizations. Training does not only teach people how to react to specific situations, but also how to respond to situations

that are not in the training manual (Roberts & Bea, 2001). Employees in HROs also learn to develop responses that can detect dangers (Roberts & Bea, 2001).

HROs invest a lot of time in reviews in order to learn from their incidents (Weick & Sutcliffe, 2001 p 41). Incident analysis helps in building an organizational memory of what happened and why, develops a science of incidents that can happen in the organization and identifies parts of the system that should have redundancies (Roberts & Bea, 2001). Cooke (2003) calls this an "incident learning system": "the collection of organizational capabilities that enable the organization to extract useful information from incidents of all kinds and to use this information to improve organizational performance over time". According to Cooke (2003), an effective incident learning system is important for continuous improvement of the capability of the Incident Management process. Without such a system, pre-cursor incidents are only visible with the benefit of hindsight. But with an incident learning system in place, an organization can prevent serious accidents and may involve into an HRO over time (Cooke, 2003). The incident briefing set up by the financial institution is good step in the direction of such an incident learning system.

Another way of becoming more aware of dangers, and training incident handlers in becoming more resilient, is by simulating an incident in the organization. Simulated incidents reinforce the idea that people must not become complacent, that the organization believes that accidents might happen, and that it worries about its ability to respond (Roberts & Bea, 2001). It also teaches people in the organization to formulate appropriate responses in new situations and gives people the opportunity to see what responses work and how, so they can locate the weak spots in their organization (Roberts & Bea, 2001).

6 CONCLUSION

In this paper we have built up a discussion that confronts a trusted principle from Organizational Learning – learning through trial and error processes – with insights from High Reliability Organizations. The paradox consists of the fact that organizational learning – at least the mutual learning aspects of it – contribute to a loosely coupled organization and a suboptimal performance. We have argued that because of the absence of trial-and-error learning in high hazard environments, HROs are more successful than Learning Organizations in terms of efficiency.

Organizations do not only need to be efficient, they need to be reliable as well. Reliability is the number one concern for HROs. HROs manage to operate efficiently while staying highly reliable because they have a certain state of mindfulness, the general term for the five distinctive qualities they possess.

Through a case study of the IT Incident Management process at a large European financial services provider, we investigated how people involved in a process of such a mainstream organization, where reliability is of great concern, can learn from HROs to balance both virtues of reliability/effectiveness and flexibility/efficiency. Our observations suggest that HROs may offer valuable insights for mainstream organizations like financial institutions on how to improve their level of mindfulness.

There are some examples of past studies that look at mainstream organizations from an HRO perspective, e.g. investment banks (Roberts & Libuser, 1993) and software firms (Vogus & Welbourne, 2003), but the principles that make a HRO highly reliable have not been examined as detailed before at non-HROs. Although this study has been carried out at the idiosyncratic context of the IT department of a large financial institution, an environment characterized by critical business processes and high awareness of the potential impact of incidents, we expect our conclusions to be applicable to other high hazard environments as well. The validation of this assumption will however require further research in these environments.

References

Aase, K. and Nybø, G. (2005). Organisational knowledge in high-risk industries: Supplementing model-based learning approaches. Int. Journal of Learning and Intellectual Capital 2 (1), 49-65.

Agar, M.H. (1986). Speaking of ethnography. Sage Publications, Beverly Hills (CA).

Central Computer & Telecommunications Agency (2000). Best practice for service support: ITIL, the key to managing IT services. The Stationary Office, Norwich (UK).

Cooke, D. L. (2003). Learning from incidents. In Proceedings of the 21st International Conference of the System Dynamics Society, New York.

Denrell, J. Organizational adaptation and loose coupling. Unpublished manuscript.

Endsley, M.R. (1997). The role of situational awareness in naturalistic decision making. In Naturalistic decision making (Zsambok, C. and Klein, G., Eds), pp 269-284, Erlbaum, Mahwah (NJ).

Hammersley, M. and Atkinson, P. (1995). Ethnography: Principles in practice. Routledge, London.

Heller, R. and Willatt, N. (1977). Can you trust your bank? Weidenfeld and Nicolson, London.

Hong, J., Lehtonen, M. and Ståhle, P. (2004). Co-evolution of knowledge and competence management and its strategic implications. In Proceedings of the Fifth European Conference on Organisational Knowledge, Learning and Capabilities, Innsbruck.

Myers, M.D. (1999). Investigating information systems with ethnographic research. Communications of the AIS 2 (23), 1-20.

Nooteboom, B. (1998). Cost, quality and learning based governance of transactions. In The changing boundaries of the firm (Colombo, M., Ed), pp 187-208, Routledge, London.

Orton, J. D. and Weick, K. E. (1990). Loosely coupled systems: A reconceptualization. Academy of Management Review 15 (2), 203-223.

Reason, J. (1997). Managing the risks of organizational accidents. Ashgate, Aldershot (UK).

Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. Organization Science 1 (2), 160-176.

Roberts, K. H. and Bea, R. (2001). Must accidents happen? Lessons from high-reliability organizations. Academy of Management Executive 15 (3), 70-79.

Roberts, K. H. and Libuser, C. (1993). From bhopal to banking: Organizational design can mitigate risk. Organizational Dynamics 21 (4), 15-28.

Rochlin, G. I., La Porte, T. R. and Roberts, K. H. (1987). The self-designing high-reliability organization: Aircraft carrier flight operations at sea. Naval War College Review 40 (4), 76-90.

Rutkowski, A. F., Van de Walle, B. and Van Den Eede, G. (2006). The effect of group support systems on the emergence of unique information in a risk management process: A field study. Proceedings of the 39th Annual Hawaii International Conference on System Sciences 1, 19a.

Van Den Eede, G., Kenis, D. and Van de Walle, B. (2004). Combining flexibility and reliability for mainstream organisational learning. In Proceedings of the 5th European Conference on Knowledge Management, pp 851-860.

Van Den Eede, G., Van de Walle, B. and Rutkowski, A. F. (2006). Dealing with risk in incident management: An application of high reliability theory. In Proceedings of the 39th Annual Hawaii Int. Conference on System Sciences, p 37c, IEEE Computer Society Washington, DC, USA.

Vogus T.J. and Welbourne T.M. (2003). Structuring for high reliability: HR practices and mindful processes in reliability-seeking organizations. Journal of Organizational Behavior 24, 877-903.

Weick, K. E. (1987). Organizational culture as a source of high reliability. California Management Review 29 (2), 112-127.

Weick, K. E. and Sutcliffe, K. M. (2001). Managing the unexpected: Assuring high performance in an age of complexity. Jossey-Bass, San Fransisco (CA).

Weick, K. E., Sutcliffe, K. M. and Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. Research in Organizational Behavior 21, 81.

Wolf, F. (2001). Operationalizing and testing normal accidents in petrochemical plants and refineries. Production and Operations Management, 10 (3), 292-305.

Wildavsky, A. B. (1988). Searching for safety. Transaction Books, New Brunswick (NJ).

Williams, P. (2002). The competent boundary spanner. Public Administration 80 (1), 103-124.