Enabling high reliability of network infrastructure;

an explorative study to map and monitor appropriate motivations and forms of knowledge that enable reliability.

Thijs Alink

OXILION
INTERNET. OBVIOUS!

UNIVERSITY OF TWENTE.

Enabling high reliability of network infrastructure;

an explorative study to map and monitor appropriate motivations and forms of knowledge that enable reliability.

Thijs Alink

Enschede, 7th of October 2010

Version 2

Cover shows: ‘Rack Servers’ by Pzado (SXC.hu)

OXILION
INTERNET. OBVIOUS!

UNIVERSITY OF TWENTE.

This study was commissioned by Oxilion B.V. and carried out under the supervision of Jeroen Tekelenburg. The first supervisor of the University of Twente is dr. Fons Wijnhoven and the second supervisor is dr. Michel Ehrenhard. Contact information can be found below.

	Client	**Student**
Name:	J Tekelenburg BSc. Financial Director Oxilion B.V.	T. Alink University of Twente School of Management and Governance Master Business Administration, IM Student number: 0211141
Address:	Boddenkampsingel 87 7514 AP Enschede P.O. Box: 575 7500 AN Enschede	Cato Elderinklaan 24 7576 EA Oldenzaal
Telephone:	+31 (0) 887 87 7678	
E-mail:	j.tekelenburg@oxilion.nl	t.alink@student.utwente.nl

	1e supervisor	**2nd supervisor**
Name:	Dr. A.B.J.M. Wijnhoven Associate Professor of Knowledge Management and Information Systems University of Twente School of Management and Governance Information Systems & Change Management	Dr. M.L. Ehrenhard Assistant Professor Strategy & Entrepreneurship University of Twente Dutch Institute for Knowledge Intensive Entrepreneurship (NIKOS)
Address:	Ravelijn Building, Room 3341 P.O. Box 217 7500 AE Enschede	Langezijds, Room LAA205 P.O. Box 217 7500 AE Enschede
Telephone:	+31 (0) 53 489 3853	+31 (0) 53 489 4531
E-mail:	a.b.j.m.wijnhoven@utwente.nl	m.l.ehrenhard@utwente.nl

MANAGEMENT SUMMARY

The internet has become a vital element in modern society and modern business. Ensuring that it functions properly has become a crucial task. The internet needs a tough infrastructure to function well. The digital economy depends on this infrastructure for sharing any type of content.

The internet infrastructure is created and managed by a variety of companies. This study focuses on one of these companies, namely the hosting provider Oxilion. The company, like any hosting provider, offers a service that allows businesses to store and publish any type of data on the internet. These businesses are in need of a reliable partner and expect that Oxilion's service is always up and running. These customer expectations pressure Oxilion to manage its complex network infrastructure extremely well. The infrastructure of Oxilion is designed to cope with failures, but it cannot handle unanticipated failures. When unanticipated failures occur, employees must be able to take appropriate action. However, what enables employees to take appropriate action? Additionally, how should this be monitored?

One assumes that by taking appropriate action (behaviour) employees can eliminate threats to reliability. Their actions are influenced by their motivation and their knowledge. An individual's attitude and perceived subjective norms (collectively called motivation) guide the way in which an individual evaluates alternative courses of action and consequently the way he or she behaves. An individual's knowledge specifies the potential range of actions that he or she can take and consequently potential behaviour.

Based on Oxilion's practical problem and the proposed assumptions, three research goals were drafted. First, this study aims to describe what knowledge and motivations are needed to create appropriate behaviour. Second, this study aims to provide a 'tool' that can be used to monitor reliability, behaviour, motivation and knowledge. Third, this study aims to describe how Oxilion can learn from the information gathered by monitoring reliability.

The study uses a concurrent transformative mixed method design encompassing six data collection methods. The research diary method is the primary method for collecting data. Data collection spanned a period of four months (April – July 2010). The length of the data collection period and its broad spectrum resulted in a wealth of data. This data was analysed descriptively and by means of the qualitative data analysis method developed by Creswell (2009). This method involves coding data.

During the analysis it became clear that not all possible interactions of Oxilion's complex and changing technology could be understood and anticipated to. As a result, employees were often

‘trouble-shooting’, meaning that they were containing the effects of incidents that had already occurred. This mode of realizing reliability requires a special configuration of motivations and knowledge. First of all, it requires appropriate containment motivations that focus on resilience. Three classes of motivations demonstrated to be especially important, namely: (1) motivations regarding diagnosis and resolution, (2) motivations regarding communication and collaboration, and (3) motivations regarding knowledge development and sharing. Second, two forms of experiential knowledge were required: (1) a complex set of understandings and experiences regarding a technology to interpreted signals of a failure correctly and (2) an acquaintance with an entity to effectively acquire information (propositional knowledge) about the diagnoses and resolution of incidents.

In order to realize high reliability, Oxilion should not only be able to create appropriate motivation and knowledge (and thereby behaviour and reliability), the organization should also to monitor any changes in the variables. Motivation and knowledge, the aspects that enable appropriate behaviour, should be monitored by a half-yearly internal survey and half-yearly assessment respectively. Both monitoring tools should be tailored to the motivations and forms of knowledge needed by Oxilion. These motivations and forms of knowledge were discussed above. The information gathered with the monitoring tools can be used to decide whether initiatives for improvement should be deployed and, if so, on what aspects these initiatives should focus.

Reliability should be monitored by archiving threats to reliability. Each threat should be registered and stored in an incident database. This information could be used to determine the reliability level of Oxilion. Additionally, the information stored in the database could be used for learning purposes. By reusing stored resolution strategies the organization could achieve more effective error-correction (single-loop learning). By innovating and combining stored resolution strategies the organization could develop new resolution strategies (double-loop learning). The insights provided by the monitoring tool might lead to an adjustment in learning style and consequently deutero learning (learning to learn).

To sum up, in order to realize reliability, Oxilion should use a tool that consists out of three sub tools: (1) an incident database to monitor reliability and facilitate learning, (2) a half-yearly internal survey to monitor motivation and (3) a half-yearly assessment to monitor experiential knowledge.

INDEX

PREFACE

How do your check your savings? How do you transfer money from your bank account? Which service do you use if you want to sell the old furniture you have stored in the attic? Who do you turn to when you want to check the news at any time of the day? How do you know which houses are fore sale in the neighbourhood you want to move to?

Most likely you do not think about how much you use the internet. And you are probably not aware of your dependence on a functioning internet connection. For most people it is obvious that the internet just works. But what if it fails? A lot of people would not be able to search for information, look-up product reviews or check the news (these are the most popular activities on the internet according to Synovate, 2009). However, the damage of individual's inability to use the internet is nothing compared to the damage suffered by some companies who experience an internet failure, because a number of companies rely heavily on the internet for its operations.

This study is all about increasing the reliability of the internet. Or, more precisely: increasing the reliability of network infrastructure. This study aims to answer the question: what would be the requirements, from a human perspective, to create a reliable network infrastructure?

This study is the last part of my master Business Administration at the University of Twente. In January 2010 I had finished all the regular courses. Therefore, I started looking for an interesting graduation assignment. The hosting branch had always intrigued me, so logically this branch formed the point to start my search. The first request I sent was to an interesting hosting provider called Oxilion. Luckily, they accepted my request. And the rest, as is commonly stated, is history.

I could not have completed the thesis with help and participation of a lot of people. First, I want to thank my supervisor at Oxilion, Jeroen Tekelenburg, for his advice, helpful insights and allowing me to develop my own assignment. Second, I want to thank my supervisors at the University of Twente, Fons Wijnhoven and Michel Ehrenhard for giving me useful feedback and pointing out issues in need of improvement. Additionally, I want to thank Larik-Jan Verschuren of Oxilion for providing me with interesting suggestions and explaining all the technical aspects of the company. Finally, I want to thank my family, friends and colleagues for their support.

Enschede, 6 October 2010.

Thijs Alink

1. INTRODUCTION

The purpose of this chapter is to introduce the context of this study, present the unit of analysis and describe the study's objective. The chapter starts by establishing why a reliable internet infrastructure is, in general, important. Next, the chapter zooms in on a group of companies that manage a part of the internet infrastructure. Often these companies are jointly referred to as: the hosting branch. One of these companies is the unit of analysis of this study. The chapter will provide a description of this company and presents their main business challenge. From this challenge a practical problem and research objective is derived.

1.1 PROLOGUE

The internet has become an indispensable element in modern society: it is infused in almost every aspect in our daily lives (Yan, Eidenbenz, Thulasidasana, Datta, & Ramaswamy, 2009). It makes "economic activity more efficient, faster, and cheaper" (Yan et al. 2009, p. 2), and broadens social interaction in unmatched ways (OECD, 2008). The internet is boosting competition, spurring the tempo of innovation and promoting reorganization of industries and businesses (OECD, 2008).

A major part of the European consumers and almost every European business is connected to the internet. Within the European Union, 50% to 82% of all households and 93% of all businesses have access to the internet (OECD, 2009) (Eurostat, 2009). On average 16% of all European businesses receive orders on-line, while 28% of all European businesses make on-line purchases (Eurostat, 2009). Bear in mind that this is a European average. The proportions vary from country to country.

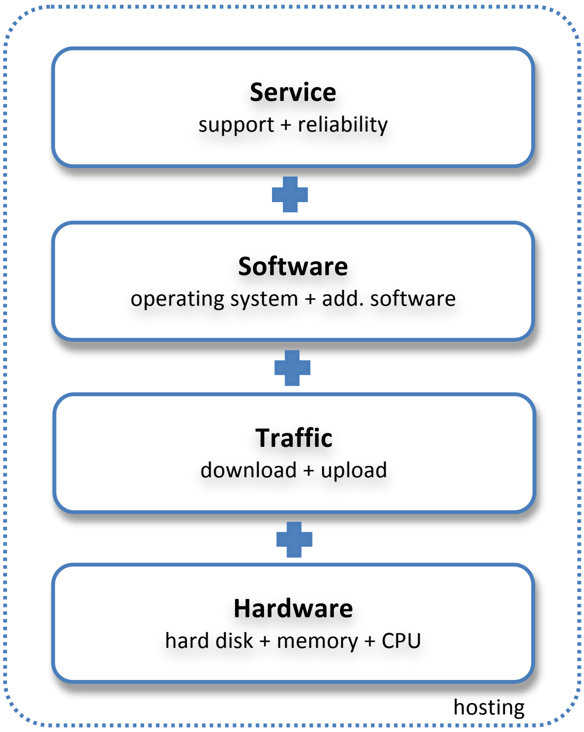
Internet has thus become a vital element in modern society and modern business. The impact of these technologies on business and commerce has been dramatic (Lucas & Sylla, 2003). But the same technologies that have enabled growth may also be a source of large disruptions (Leveson, Dulac, Marais, & Carroll, 2009). An internet failure can have major consequences for sectors that rely on an operational internet connection. Without the internet, aviation would not be possible, financial markets would not function, supermarkets' supplies would not be replenished, tax returns would not be completed and it would be impossible to manage the power grid (Huttner, 2007). Ensuring that the internet functions properly is thus a crucial task. It needs a tough infrastructure to function well (Lucas & Sylla, 2003). Barua, Pinnell, Shutter, & Whinston (1999) define internet infrastructure as "high speed and intelligent electronic networks that enable sharing of any type of content between all agents in the economy" (p. 4). The digital economy depends on this infrastructure for sharing any type of content similar to the physical economy, which depends on the road, rail, shipping and aviation network for the transportation of commodities (Chakrabarti & Manimaran, 2002).

1.2 HOSTING AND THE HOSTING BRANCH

The internet infrastructure is created and managed by a variety of companies (Barua, Pinnell, Shutter, & Whinston, 1999). This study focuses on group of companies collectively called hosting providers. Hosting providers offer 'online space' that enable individuals and business to publish any type of data and make it accessible on the internet. Some organizations use the services of a hosting provider to support critical business processes or business applications. Others use hosting to inform their customers about their organization and their services by means of a website. At some companies hosting does not only enable business, it means business. Internet companies like Amazon or eBay use hosting to power their single distribution channel: their website.

Hosting is usually described according to several characteristics, namely: hardware, traffic, software and service. These characteristics can in turn be broken down into several sub characteristics. Figure 1 depicts and describes the (sub) characteristics of hosting[1]. Hosting providers use these characteristics as a basis for their pricing policy and promotion of their product offering.

Figure 1: characteristics and sub characteristics of hosting



← **Description:** *Service* offered with hosting consists, in general, out of two elements: the level of support offered (e.g. by mail or telephone) and the level of reliability guaranteed (e.g. 95% or 99%). The level of support and the level of reliability are largely depended on contractual agreements.

← **Description:** In general, two broad *software* categories can be distinguished: an operating system (e.g. Windows, Linux) and additional software (e.g. Direct Admin, Joomla, Magento). These two categories specify (to a large degree) the functionality of a hosting account.

← **Description:** *Traffic* encompasses two elements: data that can be downloaded from and data that can be uploaded to a hosting account. Traffic is generally associated with the number of visitors an account can handle.

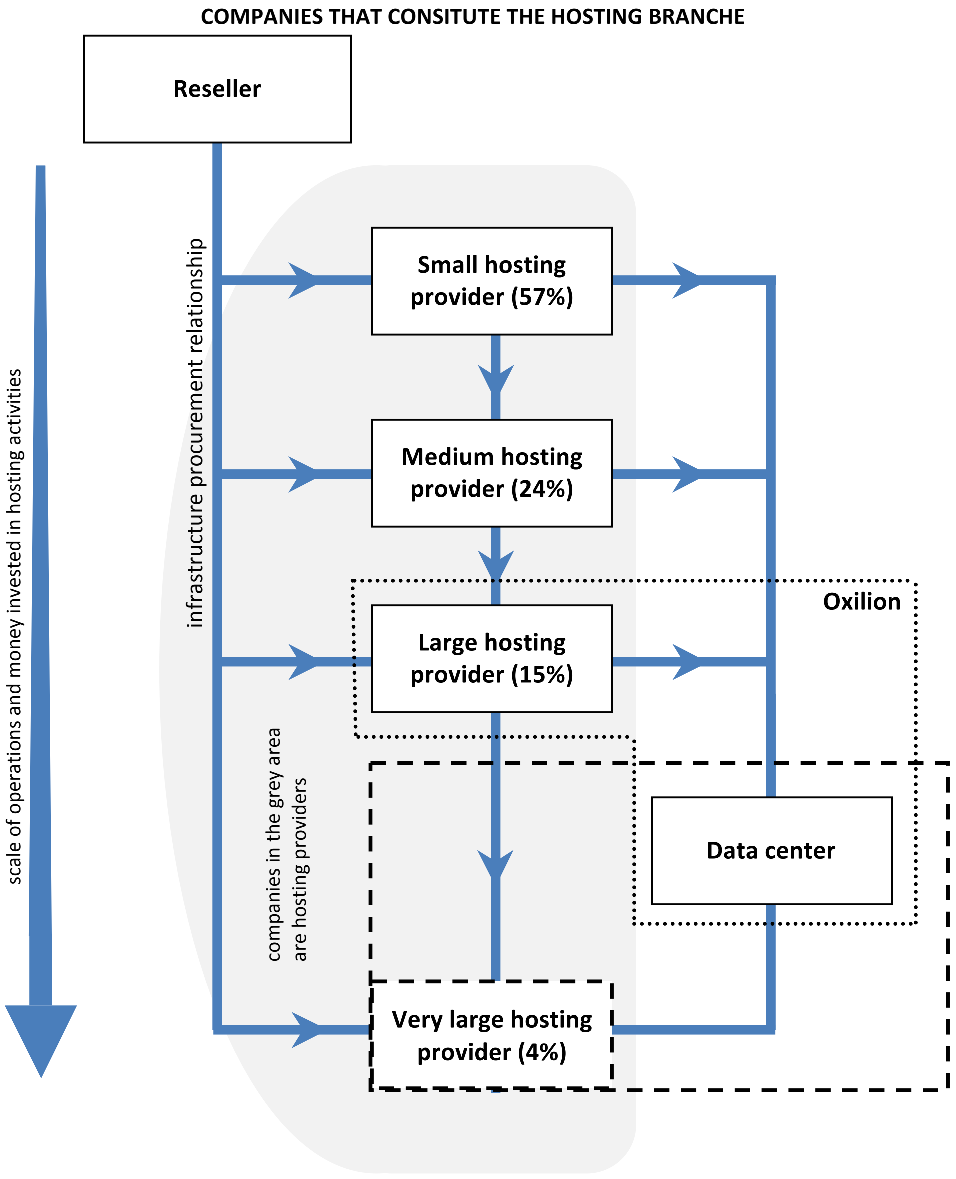
← **Description:** Often three *hardware* resources are distinguished: the hard disk (the amount of data that can be stored), CPU, and memory (which together determine the number of requests for data that can be handled at the same time).

[1] This thesis uses a self-developed model to describe hosting. Other models, such as the frequently used OSI-model, are generally aimed at describing IT-infrastructure on a technical level (e.g. the OSI-model describes how systems communicate with each other). In general these models do not include the service characteristic of hosting given that it is not directly related to technology. The figure used in this thesis is derived from multiple descriptions of hosting product offerings. In other words: it characterizes hosting along the lines that providers regard as important.

There are a lot of companies that are directly or indirectly connected to hosting (e.g. hardware manufactures, software developers, telecom providers, semi-governmental organizations). However, this study limits its description of the market to companies that offer some form of hosting. This group of organizations is generally referred to as the hosting branch. These companies can be categorized according to common stages of growth, meaning their scales of operations and money invested in hosting activities (figure 2). A short description of each company:

- A *reseller* is, as the name implies, an intermediary between a customer and a hosting provider. Most resellers buy one large hosting account, divide this account into several accounts and resell these accounts. A reseller can either be a very small hosting provider or an internet-related company that offers hosting to support their main product (e.g. web design or marketing). Resellers are only responsible for customer contact and associated tasks. Examples: TriMM, bSeen, Webton, GreenOrange.
- *Small hosting providers* are usually sole proprietorships that offer simple forms of hosting. They lease their hardware from other providers and let this provider manage the hardware. The small provider is only responsible for the software on the server and customer contact. Examples: Serveo, Hofstad Hosting, NetMatters, xYnta.
- *Medium hosting providers* are commonly general partnerships and limited companies. These providers own their hardware. They are responsible for all aspects of running a hosting company including hardware-, software- and user management. Examples: Antagonist, PC Extreme, SoHosted, Cillix.
- *Large providers* are in general limited companies. These providers have the same responsibilities as medium hosting providers. However, their product offering consists generally out of more complex products and their scale of operations and money invested far precedes medium hosting providers. Examples: Hostnet, Strato, Combell, Your Hosting.
- *Very large providers* are usually joint stock companies operating in multiple countries. They are in essence a large provider, but operate out of multiple locations that they either own or lease from a third party. Examples: LeaseWeb, Rackspace, One, Active24.
- A *data center* facilitates a reliable and protected environment for the hardware of hosting providers. It is a building equipped with (among other things) physical security, climate control and a redundant power source. A data center is, in general, responsible for managing the network infrastructure that connects the hardware of the provider to the internet. A data center is connected to the internet by multiple fast broadband connections. Examples: Equinix, EvoSwitch, BIT, TeleCity.

Figure 2: overview of companies that constitute the hosting branch, their tasks and associated knowledge


COMPANIES THAT CONSITUTE THE HOSTING BRANCHE
Reseller
Small hosting provider (57%)
Medium hosting provider (24%)
Large hosting provider (15%)
Oxilion
Data center
Very large hosting provider (4%)
scale of operations and money invested in hosting activities
infrastructure procurement relationship
companies in the grey area are hosting providers

	TASKS	KNOWLEDGE
Reseller	- customer contact (sales/support) - user management - setting up hosting accounts - tasks related to their main services	- general sales skills - general knowledge of internet/pc's - hosting account management - knowledge related to their main services
Small hosting provider	- all of the above - manage software on one or a couple of servers	- all of the above - server configuration - installing and configuring operating systems and additional installed software
Medium hosting provider	- all of the above - management of one or several racks - server maintenance and set-up - local network maintenance and set-up	- all of the above - configuring and managing servers and racks (installing and maintenance) - local network management
Large hosting provider	- all of the above - set-up and maintenance of a overarching server base that enables complex and capital intensive technologies	- all of the above - configuring and managing a servers base consisting out of multiple servers and other hardware.
Data center	- facilitating interconnectivity - intra-local network management - managing a building (security, power, fire prevention, climate control)	- internet connectivity - facility management
Very large hosting provider (= hosting provider + data center)	- all of the above	- all of the above

Comment #1: Oxilion does not fit exactly into this model. The company is a hybrid between a large hosting provider and data center. Oxilion manages multiple racks filled with servers at several locations and manages its own network but does not own a data center

Comment #2: percentages given represent proportion of the total number of providers and are estimates based on the type of business entity as registered at the Dutch Chamber of Commerce.

There are between 900 and 1100 hosting providers in the Netherlands (ISPam, 2009). Roughly 25% of all providers were established before 2000, 25% of all providers were established between 2000 and 2004, and 50% of all Dutch hosting providers were established in 2004 or later (ISPam, 2009). The vast majority of providers that operate on the Dutch market (90%) are based in the Netherlands, a small part (8%) is based in Belgium and only 2% is based outside the Netherlands or Belgium (ISPam, 2009).

There are approximately 2000 companies accredited to register a Dutch domain name (SIDN, 2010). However, this number does include non-hosting providers such as resellers and trademark companies. The Dutch domain name is, with over four million claimed names (SIDN, 2010), the fourth most popular country domain name in the world (SIDN, 2010).

The Dutch hosting market is a very segmented market in comparison to other countries[2]. A Dutch hosting provider has to compete with a lot of small hosting providers and some large providers, whereas abroad the competition comprises mainly out of large providers. However, experts think that this will gradually change. Major players in the branch expect that the Dutch market will consolidate in the upcoming years[3]. Larger hosting providers will buy smaller providers or small providers will no longer be able to compete with large providers and will cease to exist.

The hosting branch has founded several branch organizations (table 1). The branch organizations vary in number of members, sort of members and consequently in influence they could exercise. Approximately 16% of all hosting providers have joined one of these initiatives.

Table 1: Dutch hosting branch organizations

Name	***# Members***[4]	***Goal(s)***	***Type of members***
Dutch Hosting Provider Association	20	(1) Enhance ‘profile’ and ‘strategic value’ of the branch. (2) Exchange of knowledge and information. (3) Function as a spokesperson.	Mayor players within the industry and precursors
Foundation ISP Connect	51	(1) Function as a spokesperson in the media and political affairs.	Mainly small hosting providers
Foundation ISP Interest	87	(1) Function as a spokesperson when “action or participation is needed”.	Small hosting providers

[2] Derived from interviews on HostWise.nl and ISPam.nl with Con Zwinkels (Managing Director of LeaseWeb) in December 2009, Anthony Carter (CEO of Rackspace BeNeLux) in August 2008, Goran Andersson (Director Northern Europe of Amen) in May 2007.

[3] Derived from interviews on HostWise.nl and ISPam.nl with Con Zwinkels (Managing Director of LeaseWeb) in December 2009, Wouter de Vries (founder of Antagonist) in September 2007, Anthony Carter (CEO of Rackspace BeNeLux) in August 2008, Valentijn Borstlap (Director of Your Hosting) in May 2007.

[4] Retrieved on 08-09-2010.

1.3 OXILION

One of the companies operating in the Dutch hosting branch is the hosting provider Oxilion. Oxilion is a limited company based in Enschede. The provider is a hybrid between a large hosting provider and a data center. It offers hosting services to businesses that are in need of a reliable partner to store all kinds of data. These businesses do not have the knowledge to manage hosting services or do not have the funds to create a protected and reliable environment for their data.

The current two owners founded Oxilion ten years ago. They started by offering hosting to small business who searched a partner to host their website. Over the years their service portfolio changed. Oxilion now offers hosting to small-, medium- and large businesses that use the company's services to host websites, business- and telecom applications. Oxilion has achieved an average growth rate of 60% (turnover) per year in the last three years. Their growth was mainly fuelled by word of mouth. But their policy regarding marketing is changing. The company now also applies active ways to reach potential customers.

Oxilion has changed their value proposition several times to tap in to new customer segments. This process has shaped the company's current business model and consequently their current value proposition. The Financial Director described this process as following:

> "We have used several trade names in the past. Our idea was that if we came up with a new name and a new price-scheme we could attract a new category of customers. However, we found out that this also attracted a lot of customers we did not sought after. For example customers who solemnly value price, who get furious when we increase the price of our services by merely € 2.50 a year and customers who do not pay on time, or do not pay at all for that matter. After this experience we told ourselves 'we do not want to experience this ever again'. Now we are targeting customers who want to pay a bit more. By that I don't mean we are an expensive hosting provider. We are targeting customers who value our quality services and thus are willing to pay a little bit more […]. *We aim to be technically outstanding and consequently try to be a reliable partner for our customers.* […] Our customers are mainly resellers of all kind of services, such as web designing or marketing. We seek after these types of customers. They need reliability but do not want to pay an incredible large sum of money".

From the quote above one can infer two aspects of Oxilion's value proposition, namely high quality products and reliable services. The Managing Director names two other aspects of Oxilion's value proposition: being easy accessible and customer focussed. The next quote from the Managing Director provides a good example of what accessibility and customer focus entail in practice:

> "Our customers find it very pleasant that *they can just phone up* an engineer, tell him that they have just started a new campaign and notify him that they need an extra server. When they call in the afternoon and ask for an extra server, we have it up and running that same night."

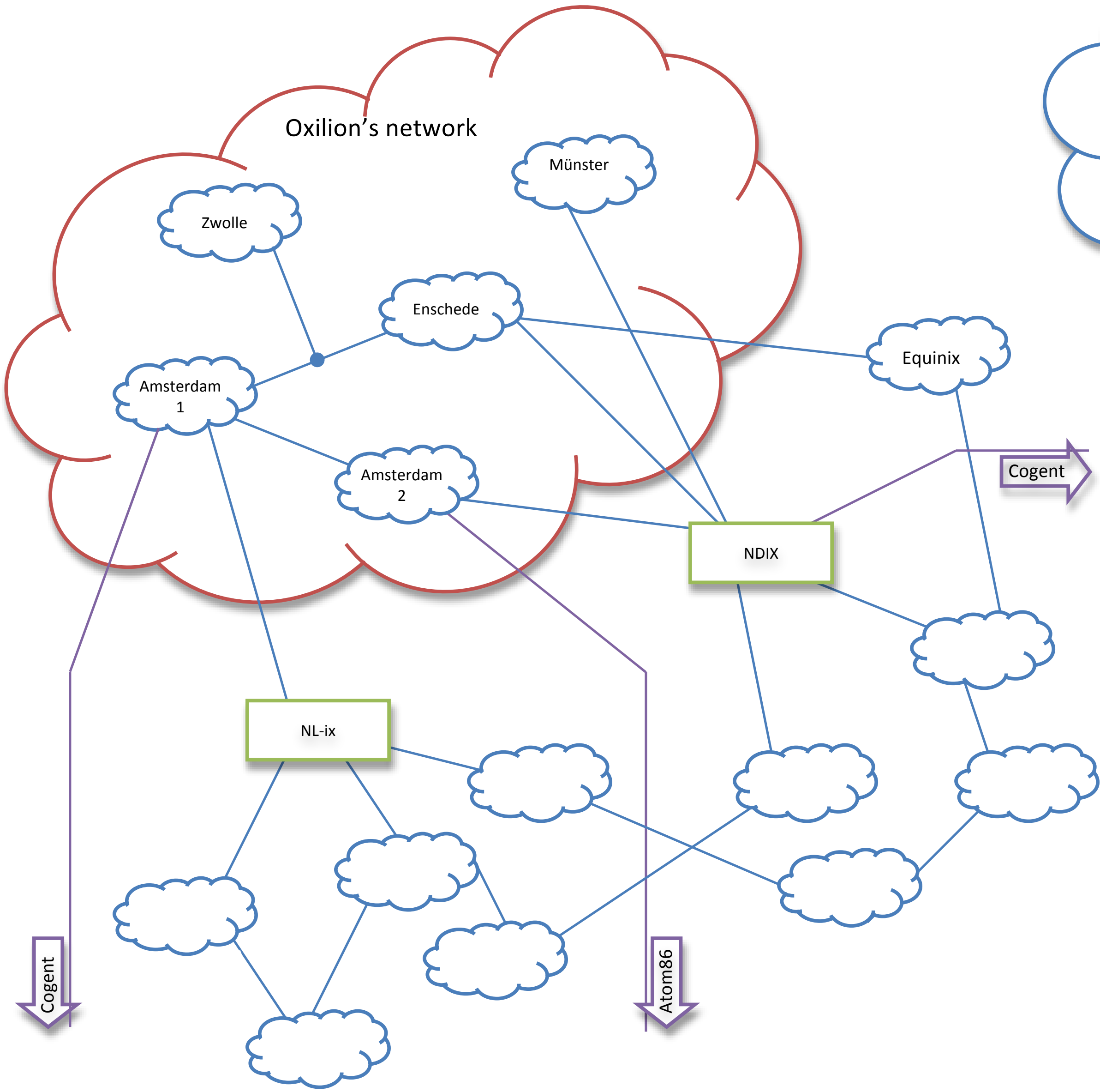
> “Our sales consultants visit our customers on a regular basis in order to keep in touch. They want to make sure that they know what is happening and keep the customer posted on new developments. I think that the way other hosting providers handle customer contact is very different. They operate out of an office. They do have contact with customers, but only by telephone. I think that *face-to-face contact* with customers is one of the things that differentiates Oxilion from competitors.”

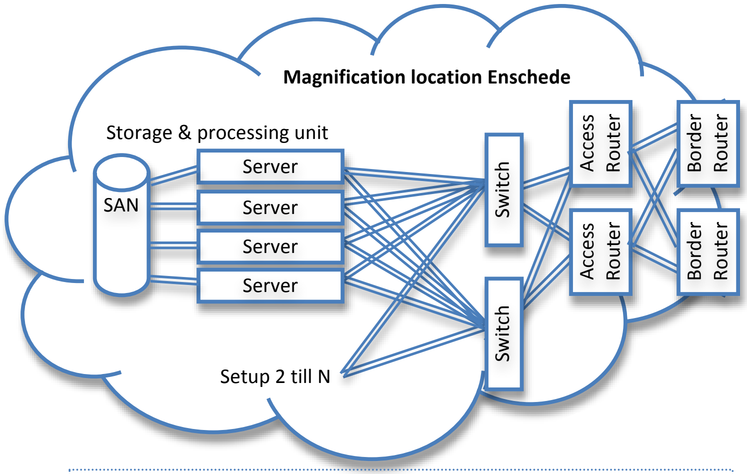
To summarize, Oxilion’s value proposition can be described as a customer focused hosting service for businesses that value a close relationship with their provider and are in need of a high quality, reliable environment to store their data.

The value proposition of Oxilion incorporates four important aspects of the company’s service. Reliability is however more important then other aspects. A customer survey (January 2010, N=324) showed that Oxilion’s customers acknowledge reliability to be the most important aspect of a hosting service. Reliability in this context means uptime. Oxilion’s customers expect that the company’s service is always up and running. Their customers include a telecommunications provider, a major online shop, an insurance company and a bank. For these and similar customers a reliable hosting service is crucial for supporting or enabling business. Hence, they cannot afford any downtime since it will have significant effect on their business. They need Oxilion’s service to be available 24 hours a day. Until now Oxilion has managed to meet this demand. The company has a track record of 99,99% uptime on a yearly basis. In order to retain this track record Oxilion cannot afford to be unavailable for more than two hours and 53 minutes on a yearly basis.

Oxilion has built a redundant network infrastructure in order to guarantee reliability. The network infrastructure of the company comprises several locations. Every location is interconnected to another location or a third party so that access to the internet is guaranteed. Each location is equipped with redundant technology. If one component fails another will take over without any downtime. The key part of Oxilion’s internet infrastructure is located in Enschede. The company aims to open up a second key location in Hengelo by the end of 2010. The second ‘key’ location allows the company to offer an even higher degree of reliability. Both locations will be each other’s equivalent. If one ‘key’ location fails, the other ‘key’ location will take over without any downtime. Figure 3 on the next page provides a description of the network infrastructure. The second ‘key’ location is not depicted.

Figure 3: Oxilion's network and connections to the internet infrastructure





🡑 **Description:** The basic 'building block' that powers Oxilion's most sold service is the storage device SAN (Storage Area Network) in combination with multiple servers. The SAN functions as a storage unit, while the servers are processing units. If a visitor requests specific data, the data is retrieved from the SAN by the server and sent to the visitor's computer. The switches distribute incoming requests for data. The access routers function as gateways to the local network, whereas the border routers (as the name implies) function as gateways for Oxilion's network. They are situated at the periphery of Oxilion's network and connect it to the rest of the internet.

🡐 **Description:** Oxilion's network (depicted as the large cloud) consists of five interconnected local networks, one local network for each physical location. Oxilion's network is connected to two internet exchanges and three IP transit services. The internet exchanges NL–ix and NDIX (depicted as squares) are basically local market places where companies like Oxilion interconnect their networks and are able to exchange traffic. IP transit services (depicted as arrows) are firms that connect Oxilion's network to the rest of the internet. Internet exchanges operate locally and connect Oxilion's network directly to other networks, whereas IP transit services operate globally and connect Oxilion's network indirectly with other networks (namely via their network). Additionally, Oxilion's network is connected to the network of Equinix. This company runs a data center as well as a network. Their network is similar to that of Oxilion.

The network infrastructure of Oxilion is initially the factor that enables reliability. It is designed to cope with a number of failures in order to realize reliability. However despite its redundancy network infrastructure could break down. Unforeseen failures could occur. These failures cannot be handled by Oxilion's systems given that these systems are only designed to handle anticipated problems. When unanticipated failures occur employees must step up. They have to use their knowledge, improvise and take action to restore systems and thereby Oxilion's network infrastructure. Employees are thus essential when network infrastructure fails.

Oxilion currently employs fourteen people, of which seven have various technical functions. Three employees offer support. The other employees are engineers that manage Oxilion's network. About half of the engineers possess a bachelor degree in information technology, the other half posses a master degree in information technology or electrical engineering. Additionally, depending on their function, the engineers have gained certificates for technologies of manufacturers such as Cisco, Dell, Microsoft, RedHat and VMware. Oxilion's directors do not only value formal education, they also value former experience. Oxilion codifies some knowledge, but most knowledge resides in employee's heads. This suggests that reliance on individuals is high. If employees leave the company, their valuable knowledge regarding the network infrastructure or specific hard- and software leaves with them. Oxilion is aware of its heavy reliance on employees. The Financial Director expressed this heavy reliance as following:

> "Hardware [referring to the network infrastructure] can be bought by anybody at HP or Dell, but it are the employees and their expertise who must make the difference".

The company is thus aware of their heavy reliance on employees. Hence, it is aware of the fact that only employees are able to handle unforeseen failures in the company's complex and changing network infrastructure. Based on this notion, Oxilion has hired employees with a lot of experience in specific software or network architecture. These employees were hired based on their background. The company assumed that if employees were experienced enough they would naturally be able to handle unforeseen failures and therefore realize reliability. Note that this is an assumption. Oxilion does not (accurately) know what (human) aspects enable its employees to take appropriate action when the reliability of the company's network infrastructure is threatened. For that reason the company would like to know what (human) aspects enable it to realize reliability. Additionally, Oxilion wants to know how it can monitor these aspects.

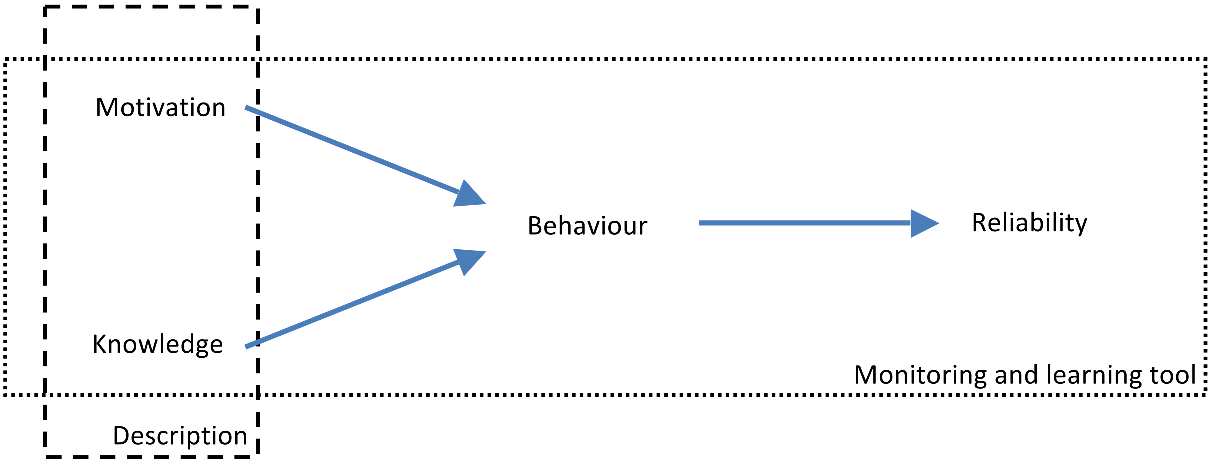
1.4 RESEARCH ASSIGNMENT

The previous section described that high customer expectations pressure Oxilion to manage its complex network infrastructure extremely well. This infrastructure needs to be reliable, meaning that it needs to be up and running 24 hours a day. The infrastructure of Oxilion is designed to cope with failures, but it cannot handle unanticipated failures. When unanticipated failures occur employees must step up. These employees must be able to take appropriate action. However, the company does not accurately know what enables their employees to take appropriate action. Moreover, Oxilion would like to know how this should be monitored.

This thesis proposes a provisional model that links reliability directly with behaviour. Behaviour is in turn linked with motivation and knowledge. The model states that by taking appropriate action (behaviour) employees can eliminate threats to reliability. Their actions are influenced by their motivation and their knowledge. An individual's motivation guides the way in which an individual evaluates alternative courses of action and consequently the way he or she behaves. An individual's knowledge specifies the potential range of actions that he or she can take and consequently potential behaviour. These relationships form the provisional basis of this study. The model (figure 4) is further explained and motivated in the second chapter.

Based on the practical problem and the provisional model, this study defines three goals. First, this study aims to describe what motivation and knowledge is needed to create appropriate behaviour. Second, this study aims to provide a 'tool' that can be used to monitor reliability, behaviour, motivation and knowledge within a specific time interval. Third, this study aims to describe how Oxilion can learn from the information gathered by the monitoring tool. Figure 4 provides a visual description of the objectives.

Figure 4: provisional research model and visual description of research objectives



In order to explore what knowledge and motivation is needed to create the appropriate behaviour one must formulate research questions that guide the study. This study poses three research questions that are closely related to its goals, namely:

RQ 1: What motivation and knowledge is needed to create appropriate behaviour that enables reliability?

RQ 2: How should motivation, knowledge, behaviour and reliability be monitored?

RQ 3: How can information acquired by the monitoring tool be used to learn and consequently improve reliability?

The first question is a normative question, while the second question is a design question. These questions imply the establishment of a 'standard' of which Oxilion's performance should be measured with a self-developed tool. The development of the tool signals a methodological change in the way the performance of the company is monitored. The third question is a descriptive question. It implies that this thesis should illustrate how a monitoring tool can contribute to knowledge development and consequently improvement of Oxilion's reliability level.

By answering the research questions, the study could contribute to practice and theory. This study could contribute to the research field of high reliability organizations by exploring high reliability issues in a SME in general, and hosting providers in particular. Both topics have received little attention from the research field. Previous studies about high reliability organizations have all explored reliability issues in large organisations. SMEs were basically ignored. By exploring reliability issues in a SME, the study could fill a gap in existing literature. Additionally, this study could create understanding about a branch on which limited literature is published. The growing dependence of society and economy on internet infrastructure marks the importance of creating understanding of reliability issues in hosting providers.

This study aims to contribute to practice by providing Oxilion with advice on what motivations and knowledge their employees need to create reliability. Additionally, this study aims to provide the company with a tool that can be used monitor reliability and learn how to improve reliability. Furthermore, this study aims to point out the importance of appropriate behaviour, motivation and knowledge to enable reliability.

2 THEORETICAL FRAMEWORK

The purpose of this chapter is to introduce the main variables of the research theory. This section describes the main variables by drawing from literature in the research field of high reliability organizations, behavioural science and knowledge management. The literature was located by performing a search on the main variables of this study (plus synonyms and related variables) in Scopus, Web of Science and Google Scholar. Key authors were identified based on times cited and the relevance of their publications[5]. The chapter sets of by introducing three (genuine) incidents that have threatened Oxilion's reliability. These incidents are used throughout the chapter to clarify the relationships between the variables. They are grounded in the theory. Next, several definitions of reliability are described of which one overarching definition is inferred. The chapter reasons that reliability is enabled by appropriate behaviour of employees. These individuals must in turn possess appropriate motivation and knowledge. These four variables (reliability, behaviour, motivation and knowledge) are linked together in one final theory. This theory forms the basis of the study.

In this chapter three (genuine) incidents are described that have threatened the reliability of Oxilion during the study. These incidents are presented in addition and parallel to the development of the model. The purpose of describing the incidents at this stage of the study is to provide an example of the relationships between the variables and to guide the development of the research model. The incidents were gathered by means of the research diary method. Employees were asked to report any incident that threatened the reliability of Oxilion and write down specific information regarding the incident in their logbook (diary). More information about the research diary method can be found in sub section 3.2.2 (page 28). The three incidents are introduced below:

> *INCIDENT 1*: The first incident concerns maintenance on one of the SANs. Engineers had to move the machine. However, before the machine could be moved the engineers had to transfer the data on the machine to another SAN. During this process a failure occurred that left the engineers unable to manage the data transfer. The potential impact of this incident was estimated to be € 11.000 annual turnover[6].
>
> *INCIDENT 2:* The second incident described here is a spam run. A spam run is a process in which an (unauthorised) user sends unsolicited bulk messages at random. Spam runs lead to a slow down in mail processing and can lead to a breakdown of mail processing if acted upon inappropriately. The potential impact of this incident was estimated to be € 115.200 annual turnover.

[5] This study especially draws from literature written by Weick and associated authors, Ajzen and associated authors, and Mingers. Weick and Ajzen were selected because they are key authors in their respective research fields. Mingers was selected given the practical applicability of his work.

[6] Estimated impact is the direct annual turnover generated by products and services installed on or executed by the system(s) involved in the incident. For clarification see page 37.

INCIDENT 3: The third incident concerns a DOS-attack (denial-of-service). A DOS-attack is an assault on a server aimed at making the server unavailable for users. It involves requesting data multiple times within a very short time period. This causes the server to overload since the server cannot handle all the incoming requests because its resources are saturated. A DOS-attack not only makes a server unavailable to users, but also slows down the network to which the server is connected. The potential impact of this incident was estimated to be € 75.000 annual turnover.

2.1 RELIABILITY

Authors have been a bit circumspect to provide a clear definition of reliability (Weick, Sutcliffe, & Obstfeld, 1999). The traditional view of reliability as defined by Hannan & Freeman (1984) and quoted by Weick, Sutcliffe, & Obstfeld (1999) is the "unusual capacity to produce collective outcomes of a certain minimum quality repeatedly" (p. 35). This definition stresses that reliability is achieved by realizing a specific level of quality time after time.

Another definition that was used by a lot of authors in early research on high reliability organizations is the term 'failure-free' (Roberts & Rousseau, 1989), (Roberts, 1990), (LaPorte & Consolini, 1991), (LaPorte, 1996). Reliability is thus seen as the number of times an error or failure is observed within a specific time period. However, this implies that the level of reliability is judged based on historic empirical or observational evidence (Rochlin, 1993). Reliability is thus determined post facto. The definition is often accompanied with statistics to support the claim that an organization is indeed highly reliable (Hopkins, 2007). Note that with this way of conceptualizing reliability it is impossible to determine in advance whether an organization is highly reliable. Also note that reliability is defined by social and perceptual criteria (Rochlin, 1993). A consumer, for example, might consider a telephone company with an outage of three days in a year reliable, while a business might consider the same company unreliable. Hence, whether a company with a specific error-rate is considered reliable depends on the perceptions of its environment.

Leveson, Dulac, Marais, & Carroll (2009) provide another definition of reliability. They draw from engineering and define reliability as: "the probability that a component satisfies its specified behavioural requirements over time under given conditions" (p. 234). Their definition is based on the likelihood that a specific level of reliability is achieved, thus reliability is not determined post facto.

From the previous discussion one can conclude that the definition of reliability used in this thesis should at least include a reference to a performance level that is maintained over prolonged period of time. Additionally, one should acknowledge that the appropriate performance level is determined by social and perceptual criteria, hence 'forces' from an organization's environment. Another aspect that can be inferred from the discussion above is that reliability can either be seen as a (immaculate) track record or the likelihood that a failure will occur based on, for example, a system's schematics. Taking all these aspects into account, reliability is defined as: consistency in meeting a specific performance level as required by an organization's environment and based on a organization's track-record and/or the chance that a lapse in reliability will occur.

In the context of a hosting provider 'consistency in meeting a specific performance level' means reassuring that their services are always available. This is called uptime. Uptime is the availability of a hosting provider's services, measured per year and denoted as a percentage. Hence, uptime can be seen as a specific reliability level. The reliability level of a hosting provider can be threatened by incidents that cause unavailability (downtime) of (a part of) its network infrastructure. Next, this section presents a part of the logbook entries of each incident (introduced at the start of this chapter) to show how incidents can threaten reliability. The words that describe a threat to reliability are denoted (R).

> *INCIDENT 1:* "The room where the SAN was placed would be renovated in a couple of weeks so we had to move the machine as well as the data on the machine. We can move data from one machine to another with VMware [a hosting management tool] without any downtime. However during the process of transferring the data from one SAN to another the management tool froze, leaving us without a way to manage the data transfer (R)."

> *INCIDENT 2:* "One of our servers was hacked this week. Due to wrong execution rights of some files a 'spammer' was able to place a script on the server. The script automatically sent thousands of e-mails. This clogged up the mail queue and caused costumers that used the server [240 in total] to experience a slowdown of their mail processing (R). A slowdown is however not our biggest concern. If spam is sent from one of our servers, the address of that server will be placed on a blacklist. This means that all e-mail sent from that server is marked as spam and consequently filtered by the receivers e-mail client. Not only that particular server would be blacklisted, our entire server park would be placed on the blacklist. Hence, nobody would receive e-mails sent with one of our servers (R)."

> *INCIDENT 3:* "On Queen's day one of our customer's servers hosted in the data center at Zwolle faced a DOS-attack. The server had to deal with almost one gigabit of traffic per second. This overloaded the server (R) as well as the connection to the data center given that the connection can only handle one gigabit per second. Due to the connection overload our other servers in the data center at Zwolle were, to some degree, not able to exchange traffic (R)."

The three incidents described above are all examples of incidents where reliability (uptime) was more or less threatened. Incident 1 describes a situation were reliability is indirectly threatened. In incident 2 and 3 reliability was directly threatened: the users experience a slowdown (incident 2) or unavailability (incident 3). Moreover, incident 2 describes also that if Oxilion's engineers did not act quickly the situation would have escalated from a slowdown to a breakdown. Situations like these can affect a provider's reliability. A provider must be able to handle these threats in order retain its track record and remain reliable as promised to customers. Whether a provider is able to handle these threats depends on the behaviour of their employees. The relationship between reliability and behaviour is explained in the next section.

2.2 BEHAVIOUR

Reliability is not an isolated concept; it is directly linked with behaviour. High reliability organizations become highly reliable by creating appropriate behaviour (Leveson, Dulac, Marais, & Carroll, 2009). Behaviour is in turn influenced by an individual's motivation (Cialdini, 2003) (Ajzen & Fishbein, 2005) and knowledge (Blatt, Christianson, Sutcliffe, & Rosenthal, 2006) (Meyer & Sugiyama, 2006). This section describes the influence of behaviour on reliability.

Jaccard & Blanton (2005) note that behaviour is in essence action. They define behaviour as: "any denotable overt action that an individual, a group of individuals, or some living system performs (p. 128). The authors stress that: "an action has a denotable ending and is performed in an environmental context in which the individual or group is embedded" (p. 128). Behaviour can thus be broken down into four core elements: "(1) an action, (2) an object or entity toward which the action is directed, (3) a setting and (4) a time" (Jaccard & Blanton, 2005, p. 131).

In order to show the relationship between reliability and behaviour this section continues with the incidents described in the previous section. The logbook entries depicted below describe which behaviour employees showed to eliminate the threats to reliability. In the examples action is coded (A), while the object or entity towards which the action was directed is coded (EO). Note that, for the sake of simplicity, only behaviour of Oxilion's employees is coded. The other two elements of behaviour (setting and time) were regarded as irrelevant in the context of this study and are therefore not coded.

> *INCIDENT 1:* After I discovered that the tool wasn't working correctly a colleague and I checked (A) the logs (EO) of the server that processed the transfer. We found messages stating that the server was out of memory. We called (A) the support desk of VMware (EO). They confirmed what we already thought: the data transfer required more memory than was at that time available on the server and the only way to free up more memory was to clear another server."

> *INCIDENT 2:* "Our monitoring tool detects and reports large mail queues (>500). We received a report from the tool, so we immediately checked (A) the mail queue (EO) for any spam. When we confirmed (A) that there was indeed a spam run (EO) going on we searched (A) the server (EO) for the script that was sending the spam. We deleted (A) the script (EO), cleared (A) the mail queue (EO) and corrected (A) the execution rights of the files (EO) that allowed the spammer to place the script in the first place"

> *INCIDENT 3:* "We received a report that a couple of services weren't working correctly. In addition to the report a customer called telling us that his server wasn't working. We checked (A) the monitoring tools (EO) and that's how we discovered that one of the servers suffered from a DOS-attack. Luckily Engineer A was on 'repair service'. He 'null-routed' (A) all traffic to the server (EO). This means that all traffic to the server is simply thrown away so that the server does not have to handle any requests. Hence, the server was no longer overloaded and it could be restarted. To prevent an overload of the connection from reoccurring the engineer reduced (A) the connection of the server (EO) to 1/10 of the original. The other servers could then use the remaining 9/10."

The examples describe various actions taken to eliminate threats. The second incident is however the one that is the most rich in detail. In this example the actions taken by the engineer were: checking, searching, deleting and correcting. The objects towards which the actions were directed were respectively: the mail queue, the script (two times) and files with wrong execution rights.

This section described that appropriate behaviour enables reliability. However, the engineers in the examples did not show appropriate behaviour automatically. They showed appropriate behaviour because they had appropriate motivation (and knowledge) to do so. The next section explains the influence of an individual's motivation on behaviour.

2.3 MOTIVATION

This thesis draws from Ajzen & Fishbein's (2005) theory of reasoned action in order to explain the relationship between motivation and behaviour. Ajzen (1991) defines motivation as an "individual's intention to perform a given behaviour" (p. 181). The theory of reasoned action suggests that two motivational factors impact whether one is intended to show specific behaviour, namely: attitude and subjective norms.

The first factor that determines an individual's motivation is attitude. Kruglanski & Stroebe (2005) note that there is considerate diversity in how attitude is defined. Nevertheless, any definition of attitude refers al least to its evaluative and dispositional nature (Jaccard & Blanton, 2005). Attitude could thus be defined as an evaluative disposition. However, an important addition to this definition is that 'disposition' refers to a disposition to behave in a certain way (Jaccard & Blanton, 2005). Therefore, attitude is defined as: an evaluative disposition to behave a certain way. The addition of 'to behave a certain way' is important because it signals that attitude impacts behaviour. The strength of the impact of attitude on behaviour is influenced by a person's belief of attaining a desired goal (Kim & Hunter, 1993). The stronger a person perceives that a specific attitude will bring about a desired goal the more likely it is that he will show the appropriate attitude.

The second factor that determines individual's motivation is subjective norms. Subjective norms are socials pressures from important persons to show specific behaviour as perceived by an individual

(Rivis & Sheeran, 2003). Ajzen & Fishbein (2005) distinguish between two types of subjective norms, namely: injunctive and descriptive. An injunctive norm is "what people typically approve or disapprove" (Cialdini, 2003, p. 105), whereas a descriptive norm is "what people typically do" (Cialdini, 2003, p. 105). Both forms of norms impact behaviour. Descriptive norms impact behaviour by providing confirmation as to what behaviour is likely effective (e.g. everybody is doing 'it' in this fashion, thus it must be sensible to do 'it' like this). Injunctive norms impact behaviour by providing evidence of what behaviour will probably be liked or disliked. Naturally, the stronger an individual perceives social pressure (from either injunctive of descriptive norms) the more likely it is that he or she will show the appropriate behaviour.

An individual's motivation is thus the function of attitude and perceived subjective norms. Enabling high reliability, however, requires specific motivations. These motivations set high reliability organizations apart from organizations that are not highly reliable (Leveson, Dulac, Marais, & Carroll, 2009). Weick & Sutcliffe (2007) mapped individual's motivations in high reliability organizations. The authors propose that the members of an organization should adopt these motivations to enable reliability. Weick & Sutcliffe (2007) categorize these motivations into two main categories named anticipation and containment. The authors propose that the interaction between anticipative and containment motivations allow high reliability organizations to manage a wide range of unexpected events.[7]

The motivations in the anticipation category focus on prevention (Blatt, Christianson, Sutcliffe, & Rosenthal, 2006). Weick & Sutcliffe (2007) describe that anticipation entails paying close attention to weak signals for problems. Weak signals have to be noticed and their unique information must be retained and not lost in category. High reliable organizations counter the loss of information (simplification) by encouraging interaction between people with different backgrounds and expectations (Burke, Wilson, & Salas, 2005). Additionally Weick & Sutcliffe (2007) describe that people in high reliability organizations need to remain aware of the current status of operations and foresee the implications for future functioning. Together, the previous described motivations enable the organization to notice failures, foresee the consequences of a failure and stop unwanted effects from developing.

It is important to note that high reliability organizations are not error-free, high reliability organization are not disabled by errors (Hopkins, 2007). They are not disabled by errors due to the

[7] Weick & Sutcliffe (2007) have transformed the motivations to anticipate and contain failures into five principles in order to place them in a practical context. Together these principles create a mindful infrastructure, which leads to the capability to discover and manages unexpected events, which in turn leads to reliability. For the sake of simplicity this study does not use the notion of principles, but sticks to calling them motivations.

motivations in the containment category. These motivations focus on resilience (Blatt, Christianson, Sutcliffe, & Rosenthal, 2006). They are mainly aimed at containing the unwanted effects after a failure has occurred and are aimed at improving the ability to recover from a failure (Weick & Sutcliffe, 2007). High reliability organizations create large and varied response repertoires to cope with failures, learn quickly and shift leadership to people who are likely to be able to solve problems at hand (Weick & Sutcliffe, 2007).

In short, anticipative motivations and containment motivations together guide behaviour to realize reliability. However, high reliability organizations may exhibit varying degrees of both types of motivations, there is no predefined ideal set-up (Hopkins, 2007). The description provided above should thus be regarded as a guideline, not as a plan that every organization should adopt in order to enable reliability.

This section returns to the examples of incidents that have threatened the reliability of Oxilion in order to show the relationship between an individual's motivation (attitude and subjective norms) and behaviour in practice. Note that the motivations described below are all examples of containment motivations. The motivations were aimed at containing the unwanted effects of failures. The engineers have not described their motivations as such, their motivations can however be derived from their logbook entries. The logbook entry of the first incident is an example of how attitude can influence behaviour.

> *INCIDENT 1:* "Our strong suspicion of the problem had to be confirmed (were we sure it wasn't a bug in the system?). Moreover, we also had to make sure that our solution was correct."

From the logbook entry one can deduce that engineer had a positive attitude towards the quality of his work. To be more precise: the engineer held it important to check (disposition) the analysis as well as the solution because he wants to be sure (goal). As a consequence he regarded it important (evaluation) to call (behaviour) the manufacturer for confirmation. The second incident provides an example of two injunctive norms:

> *INCIDENT 2:* "Our monitoring tool reported a mail queue of over five hundred e-mails. We intervened immediately and were therefore fast enough to prevent black-list listing"

From the incident mentioned above two injunctive norms can be deduced, namely: (1) react quickly to failures and (2) prevent further damage. Both norms are examples of social pressure. In this specific case, the engineer perceived that the norm is to react quickly and prevent further damage because customers and colleagues approve of this reaction and will likely disapprove of a slow reaction or even no reaction at all. The engineer is therefore motivated to act in this specific way.

The third incident reveals two attitudes, namely a positive attitude towards learning and sharing knowledge.

> *INCIDENT 3:* "I got the instructions from Engineer A, so that next time I can handle problems like this myself. I stored the instructions in my own knowledge database. When I have got enough information I write a 'manual' and publish it on the company's internal wiki."

One can analyse the logbook entry of the third incident in the same way as the logbook entry of the first incident. The engineer learns from colleagues and shares information because it contributes to his personal development as well as that of his colleagues (goals). He therefore judges it important (evaluation disposition) to write down instructions and publish them (behaviour).

This section described that appropriate motivation guide employees to show appropriate behaviour, which in turn enables reliability. However, appropriate motivation is not the only factor that enables behaviour. An individual must not only be motivated to show appropriate behaviour, he must also be capable of doing so. An individual's knowledge specifies whether an individual is capable to show specific behaviour. The next section explains the influence of knowledge on behaviour.

2.4 KNOWLEDGE

High reliability organizations are heavily reliant on employee's individual knowledge (Sullivan & Beach, 2009). This heavy reliance on individual's knowledge originates from the challenge of managing complex systems. Interaction between components of the organization's systems cannot be completely planned, understood and envisaged in advance (Leveson, Dulac, Marais, & Carroll, 2009). It comes down to employees who, when a failure is detected, have to improvise and address their knowledge to restore reliability (Blatt, Christianson, Sutcliffe, & Rosenthal, 2006). Employees thus use knowledge to employ activities (behaviour). This notion is also expressed by Alavi & Leidner (2001) who describe that knowledge can be viewed as "a capability with the potential for influencing future action" (p. 111). The word 'potential' signals that knowledge limits what actions a person can take. Hence, knowledge specifies the potential range of actions. Whether a person shows the appropriate actions depends on his or her motivation (as was explained in the previous section).

Until now, knowledge is treated as a one-dimensional concept. There are however various forms of knowledge. Mingers (2008) introduced a taxonomy of knowledge that provides a representation of the various meanings of 'knowing'. He argues that existing conceptualizations of knowledge are monovalent and developed a taxonomy based on four dimensions: (1) the object of knowledge, (2) the source of knowledge (3) the way knowledge is articulated and (4) the manner in which knowledge is warranted. Based on these dimension he identified four types of knowledge:

propositional, experiential, performative and epistemological knowledge. Next, the four forms of knowledge are discussed. Table 2 provides an overview.

Table 2: forms of knowledge (adopted from Mingers 2008)

Type of knowledge	*Object of knowledge*	*Source of knowledge*	*Form of representation*
Propositional I know it is raining I know there is a train at 3.00 I know there is some ate the door	Sates of affairs in the physical and social word *To know that x*	Direct perception, receipts of information, communications, the media	Generally explicit and propositional, although some may be tacit
Experiential I know her well I know the feeling I know I left my key there I know how the system works	People, places, events we know through personal experience. *To know x*	Personal experiences	Memories, some aspects of which may be tacit and embodied
Performative I know how to ride I know how to read an X-Ray I know how to present	Skills, abilities and competences *To know how to do x*	Personal experience, learning, training	Embodied
Epistemological I know what black holes are I know linear algebra	Reasons for the (non-) occurrence of things and events. *To know why x*	Formal methods of discovery, for example, in science	Explicit, discursive, 'objective', open to debate.

The first form of knowledge is propositional knowledge. Propositional knowledge is simply information (Wijnhoven, Schuur, & Timmer, 2010). Information can be a direct perception of something or something about which one is told. Individuals determine based on the information that is available to them if they should act (Blatt, Christianson, Sutcliffe, & Rosenthal, 2006). Hence, whether people show behaviour rests thus ultimately on information (Ajzen & Fishbein, 2005). The second form of knowledge is experiential knowledge. This is to have a personal understanding, feeling or belief about an object or entity. The depth of the experiential knowledge concerned is very variable. The source of this form of knowledge is personal experiences. The third form of knowledge, performative knowledge, goes beyond knowing something by experience since it involves a kind of physical competence. For example: knowing how to ride a bike. Note that it is to know how to ride a bike, not riding itself (which is behaviour). Like experiential knowledge, personal experience is also the source of performative knowledge. However, with performative knowledge these experiences generally involve some from of explicit training, while with experiential knowledge these experiences generally involve an acquaintance with something or a set of complex understandings of something. Epistemological knowledge, the last form of knowledge, is having a deeper understanding of things as to why something is as it is. Minger's (2008) also includes in this category scientific knowledge.

In order to show the relationship between knowledge and behaviour in practice, this section returns to the three incidents. Oxilion's engineers used different forms of knowledge to eliminate threats to reliability. In the logbook entries depicted below each form of knowledge is coded. Propositional knowledge is coded (PR), Experiential knowledge is coded (EX), performative knowledge coded (PE) and epistemological knowledge is coded (EP).

> *INCIDENT 1:* "[The knowledge to solve the problem] partially stemmed from experience (EX). However, we also attended a VCP-course (VMware Certified Professional) (EP) where we learned how to install and configure VMware, and consequently where to find the logs. Moreover, we know from experience that the support desk of VMware reacts very fast to a request for help (EX). It would thus be futile to spend a lot of time looking for a solution (PR) ourselves when the WMware support desk can provide it very fast for us."
>
> *INCIDENT 2*: "I knew how to handle a spam run from experience (EX), especially that of Linux [operating system] and Plesk [control panel]."
>
> *INCIDENT 3*: "I learned how to do this from experience (EX). However, when I had to do the 'null-routing' myself [instead of Engineer A], I would not be capable to do so. I would have to search for a solution on Google (PR) or ask Engineer A (PR). Eventually I would have found a solution. However, Engineer's A expertise (EX) on this particular topic certainly sped up solving the problem. We were lucky that he was on 'repair service'.

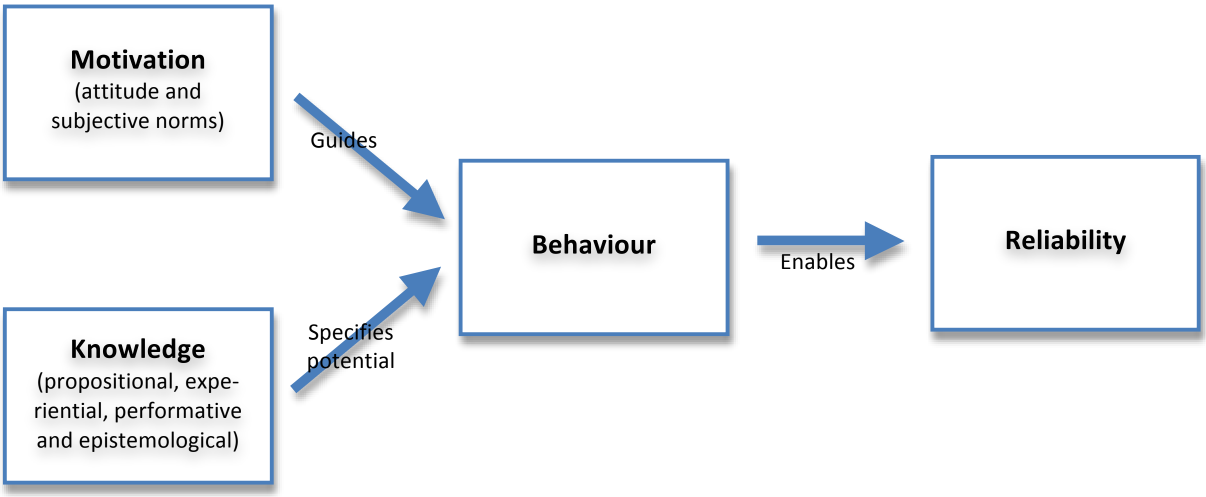
The logbook entry of the first incident is the most 'rich' in detail. In this logbook entry the engineer referred to three types of knowledge. To start with, he referred to experience, by which he means knowledge gained during previous experiences with a specific technology, hence: experiential knowledge. He also mentions a course that he and his colleague took. This can be regarded as epistemological knowledge. Next, he reveals that he knows from personal experience that the response time of the VMware support desk is very short. This is thus experiential knowledge. Lastly, the engineer refers to propositional knowledge, namely the information given by the support desk.

The example clearly shows that knowledge influences action. Had the technician for example not known that the response time of the helpdesk is very short, he might have taken alternative action. Moreover, in his logbook entry he clearly refers to an alternative action, namely looking for the solution himself. Hence, his knowledge specified the potential range of actions that the employee could take to enable reliability. This is also illustrated by the logbook entry of the third incident. The engineer describes that he is not capable to perform a specific action that would have eliminated the threat. In this case, his knowledge thus limits his potential behaviour. If he had known how to solve the problem he had not asked Engineer A, but instead implemented the solution himself. In this second example, knowledge also specified the potential range of actions that the employee could take to enable reliability.

2.5 WRAP UP

The previous sections described that reliability, which is a specific performance level as required by an organization's environment, is influenced by behaviour. By taking action employees can eliminate threats to reliability. Their actions are influenced by their motivation and their knowledge. An individual's attitude and perceived subjective norms (collectively called motivation) guide the way an individual evaluates alternative courses of action and consequently the way he or she behaves. An individual's knowledge specifies the potential range of actions that he or she can take and consequently potential behaviour. The relationships between reliability, behaviour, motivation and knowledge are depicted in figure 5.

Figure 5: research model


Motivation
(attitude and subjective norms)
Guides
Knowledge
(propositional, experiential, performative and epistemological)
Specifies potential
Behaviour
Enables
Reliability

3 METHODOLOGY

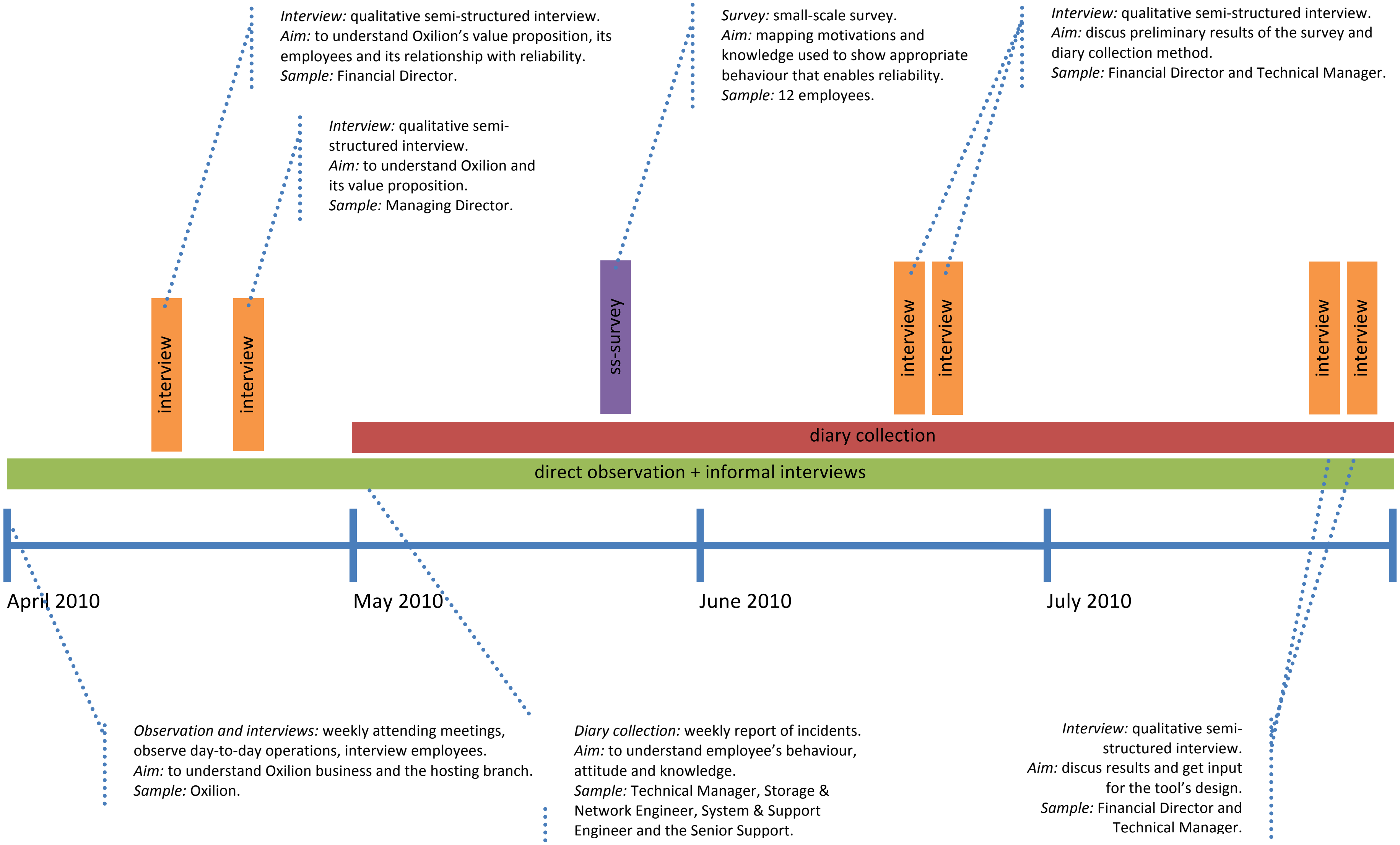
The purpose of this chapter is to describe the study's design, its data collection methods and data analyses methods. The first section substantiates why a mixed method approach was chosen over other methods. Additionally, the first section provides a general overview of the research design. The second section describes the five data collection methods included in the study. This section describes per data collection method how data was sampled, measured and collected.

3.1 MIXED METHOD CONCURRENT TRANSFORMATIVE DESIGN

This master thesis uses the mixed method research approach. This approach combines both qualitative and quantitative forms of research (Creswell, 2009). The mixed method approach offers three advantages compared with qualitative and quantitative methods: (1) the ability to triangulate findings, (2) a more comprehensive breadth of understanding and (3) deeper breadth of understanding (Johnson & Onwuegbuzie, 2004). Hence, due to its mixed nature, the outcome of a mixed method approach is usually stronger then when one uses only the quantitative or qualitative research approach (Creswell, 2007), (Johnson, Onwuegbuzie, & Turner, 2007). Therefore, this study adopted the mixed method approach. Bear in mind that in some studies the weight of quantitative and qualitative methods might not be equally balanced: a study might accentuate one or another (Creswell, 2009). This study emphasizes qualitative methods.

This study has chosen a concurrent transformative mixed method design. This design is characterized by two factors, namely: (1) its implicit use of a theoretical framework (or perspective) and (2) its concurrent data collection (Creswell, 2009). The theoretical framework that guides the study encompasses theory from the research field of high reliability organizations, knowledge management and behavioural science. Several concepts derived from these research fields were incorporated into one model. This model formed the basis for the input of the data collection methods. In total five types of data collection methods were used of which one was quantitative and four were qualitative. Three data collection methods were used concurrently, namely the diary collection method, direct observations and informal interviews. The other data collection methods (small-scale survey and semi-structured interviews) were not held simultaneously. Data collection spanned a period of four months (April – July 2010). The length and broad spectrum of data collecting resulted in a wealth of data: 48 diary responses, 20 observed weekly meetings, 12 survey responses, six semi-structured interviews and numerous informal interviews. The next section provides a more thorough picture of how this data was collected and analysed. Figure 5 provides an overview of the research design.

Figure 5: research design



Interview: qualitative semi-structured interview.
Aim: to understand Oxilion's value proposition, its employees and its relationship with reliability.
Sample: Financial Director.

Interview: qualitative semi-structured interview.
Aim: to understand Oxilion and its value proposition.
Sample: Managing Director.

Survey: small-scale survey.
Aim: mapping motivations and knowledge used to show appropriate behaviour that enables reliability.
Sample: 12 employees.

Interview: qualitative semi-structured interview.
Aim: discus preliminary results of the survey and diary collection method.
Sample: Financial Director and Technical Manager.

Observation and interviews: weekly attending meetings, observe day-to-day operations, interview employees.
Aim: to understand Oxilion business and the hosting branch.
Sample: Oxilion.

Diary collection: weekly report of incidents.
Aim: to understand employee's behaviour, attitude and knowledge.
Sample: Technical Manager, Storage & Network Engineer, System & Support Engineer and the Senior Support.

Interview: qualitative semi-structured interview.
Aim: discus results and get input for the tool's design.
Sample: Financial Director and Technical Manager.

3.2 SAMPLE, MEASUREMENT AND DATA COLLECTION

As mentioned in the previous section, this study used five methods to collect data, starting with:

3.2.1 Direct observation and informal interviews

The researcher observed day-to-day operations and attended weekly meetings with all of Oxilion's employees. In these meetings Oxilion's employees discussed daily operations and upcoming events or projects. Oxilion held these meetings in order to inform every employee of 'what was happening' beyond their own department and in order to get everybody on the same page. In addition to the weekly meetings the researcher held numerous informal interviews. These were usually short conversations about daily operations. The weekly meetings and the informal interviews enabled the researcher to understand the unit of analysis and the study's context. This was regarded as very important given that it would improve the ability to interpret the data gathered with each method. Hence, both methods (direct observation and informal interviews) were not (directly) aimed at answering one of the research questions. They were aimed at getting insights in the company and the hosting branch. The informal interviews and direct observations were not transcribed nor analysed.

3.2.2 Research diary

The third data collection method used in this project is a qualitative research diary. A diary allows the researcher to unobtrusively monitor every-day activities over a specific time period (Symon, 2004). In this case, the diary method was used to map employee's behaviour, knowledge and motivation during an incident. The goal of the method was thus to answer research question one (to be able to provide a description of appropriate motivation and knowledge).

The researcher selected four employees for the qualitative research diary method, namely: the Technical Manager, the Storage & Network Engineer, the System Support Engineer and the Senior Support. These employees were selected for two reasons: (1) they were all likely to notice possible incidents that could form a threat to operations and (2) it was likely that they would notice different threats and see different consequences given that they occupied different positions within the company, thus improving the range of incidents reported.

Each selected employee was asked to describe three things: (1) describe the incident that formed a threat to reliability (2) describe the tasks performed to eliminate the threat and (3) describe were you learned how to deal with the threat (solve the problem). Hence, the questions were aimed at discovering the nature of the incident, employee's behaviour and employee's knowledge respectively. Motivation was not included as a question since the researcher regarded it unlikely that the selected employees would be able to define their motivations. Instead, employee's motivations were derived from the answers to the other questions. In answering the first question participants were encouraged to elaborate on their answer by describing how long a threat occurred and what kind of customers were affected. This enabled the researcher to make an assessment of the impact of a threat.

Data collection spanned a period of three months (from early May to the end of July 2010). The researcher planned a ten-minute appointment in every participant's electronic agenda. At the end of the week each selected employee received automatically a message asking him to fill in his or her diary. The employees sent their diary entries to the researcher by e-mail. If the researcher did not receive an entry he would send an e-mail to the employee concerned in which he asked for a response. In total the researcher obtained 48 responses over a period of 12 weeks. This translates to a 100% response rate. 49 incidents were reported. On average four incidents were reported per week. Figure 6 depicts participant's response and figure 7 the number of incidents reported per week. The results of the research diary can be found in Appendix A.

Figure 6: overview of the participant's response per week

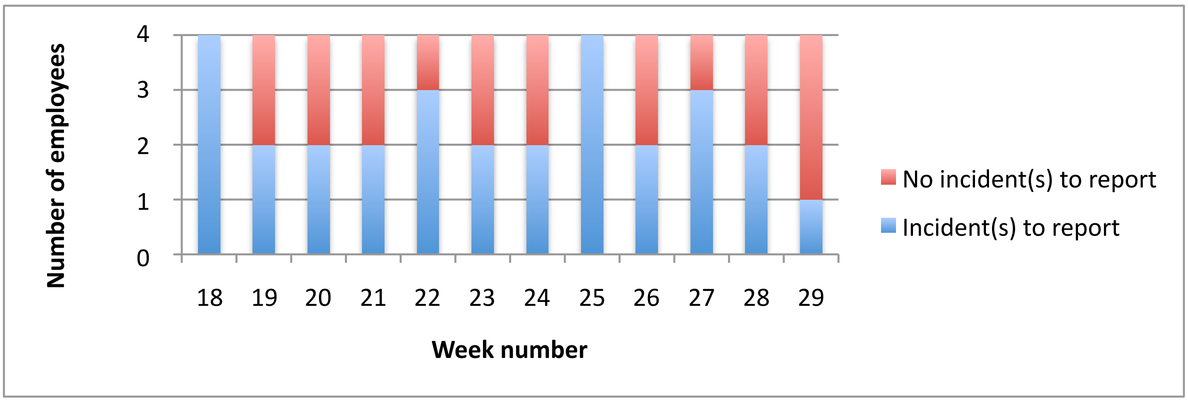
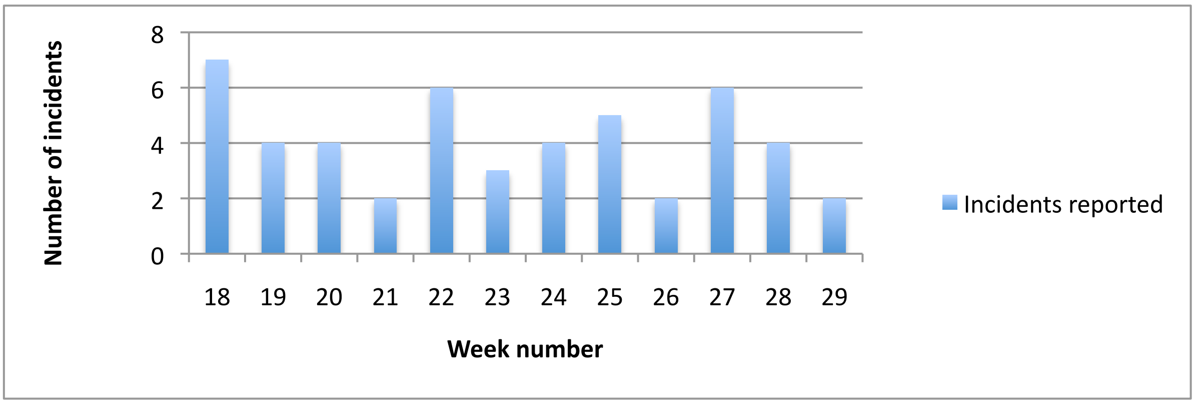


Figure 7: overview of number of incidents reported per week



The qualitative data analysis method developed by Creswell (2009) was used to analyse the gathered data. This is a linear hierarchical approach involving multiple levels of analysis. Data was coded using a combination of predetermined and emerging codes. The nature of the incidents was coded with use of emerging codes while knowledge was coded using predetermined codes based on the taxonomy of Mingers (2008). Behaviour and motivation was coded using emerging and predetermined codes. The predetermined codes of behaviour were based on the ITIL process descriptions and Jaccard & Blanton's (2005) four elements of behaviour. The predetermined codes of motivations encompassed a categorization of attitudes, injunctive and descriptive norms (as described in the theoretical framework).

3.2.4 Small-scale survey

At the end of May a small-scale internal survey was conducted. The survey was used to map motivations and knowledge used to show appropriate behaviour. Hence, it contributed to answering the first research question.

The survey assessed what motivations would be needed by a provider to achieve high reliability. The items used were based on Weick & Sutcliffe's (2007) audits. The survey consisted of six sets of on average of ten statements, each set assessing a different motivation. Employees were asked whether they agreed or disagreed with a statement (using a five-point Likert scale).

All employees of Oxilion were informed about the survey during a weekly meeting. After the meeting they received an e-mail with the internet address of the survey and supplementary text stating the purpose of the survey. Participants were also informed that participating was anonymous. The participants had a week to fill out the survey. At the end of the week all participants received an e-mail reminding them to fill out the survey. The survey was conducted with Google Docs Forms. In total 12 employees responded. This translates to a 100% respond rate. The analysis of the survey was limited to a descriptive analysis given the limited number of participants. Each set of questions concerning one specific motivation was transformed into a simple scale ranging from one to a five. Items where Oxilion scored extremely high were further investigated and used as input for upcoming interviews. The results of the internal survey can be found in Appendix B

3.2.5 Qualitative semi-structured interviews

Multiple interviews were conducted throughout the study. The advantage of interviewing, compared to previously mentioned methods is that one can explore a topic thoroughly and that one can steer the line of questioning (Creswell, 2009). The aim of the interviews was threefold: (1) discuss the results found in the small scale-survey, (2) explore the issues behind the results of the small-scale survey and the diary research method and (3), explore what could be an appropriate tool to monitor reliability. The interviews contributed to answering the first and second research question.

Three rounds of two interviews were conducted during the study. The first round of interviewing was conducted with the Financial Director and the Managing Director. These interviews were planned early on in the study and were aimed at understanding Oxilion, its value proposition, its employees and its relationship with reliability. The second round of interviews was conducted with the Financial Director and the Technical Manager. During these interviews the (preliminary) results of survey and the diary method were discussed. The aim of the interviews was to get clarification on the (preliminary) results of both methods. The last round of interviews (again with the Financial Director and the Technical Manager) was mainly aimed at getting input for the design of the monitoring tool, although some results were discussed. The interviews lasted between 34 and 46 minutes, with an average of 40 minutes. The interviews were recorded and transcribed verbatim.

Table 3 provides an overview of the gathered data. Two methods (direct observation and informal interview) are not depicted given that these methods were not transcribed nor analysed.

Table 3: overview of gathered data classified by staff member

	Interview	**Survey**	**Diary (logbook)**
Managing Director	X	X	
Financial Director	XXX	X	
Sales Manager		X	
Sales Consultant 1		X	
Sales consultant 2		X	
Technical Manager	XX	X	X
Storage & Network Engineer		X	X
Research & Development Engineer		X	
Software Engineer		X	
Senior Office & Support		X	X
Office & Support 1		X	
Office & Support 2		X	
System & Support Engineer		X	X

Comment: the number of crosses represents the number of times an employee was included in the data collection method stated at the top of the respective column.

4 DATA ANALYSIS

The purpose of this chapter is to present the findings of this study and discuss several observations. The chapter is structured along the lines of the main variables of the theoretical framework (reliability, behaviour, motivation and knowledge). Each variable is covered in a separate section.

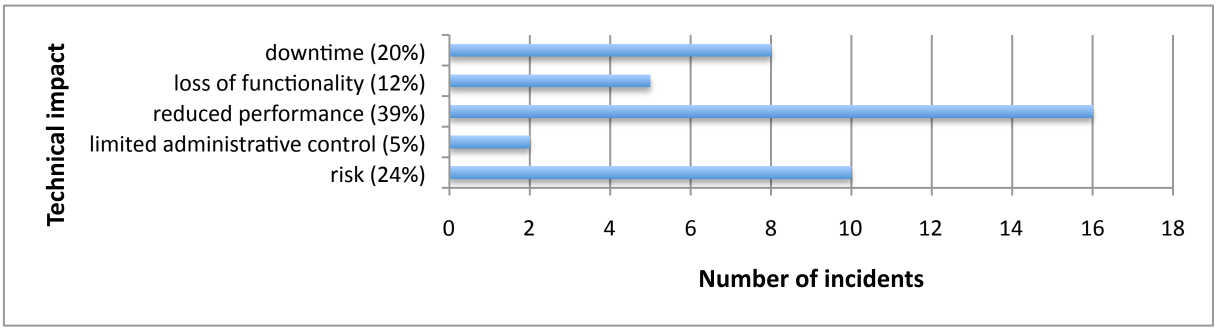
4.1 RELIABILITY

Reliability was defined in the theoretical framework as: "consistency in meeting a specific performance level as required by an organization's environment and based on an organization's track-record and/or the chance that a lapse in reliability will occur." The definition clarifies that, in the context of a hosting provider, a provider can be considered reliable if it is able to meet and maintain a specific performance level as required by their customers.

The performance level of a provider can be threatened by incidents. Incidents are events, problems or situations that threaten the availability of a provider's services to some degree. During the three months that data was collected (by means of the diary collection method) 41 incidents were submitted. The degree to which these incidents threatened reliability was described along two dimensions: (1) the technical impact of incidents and (2) the financial impact of incidents.

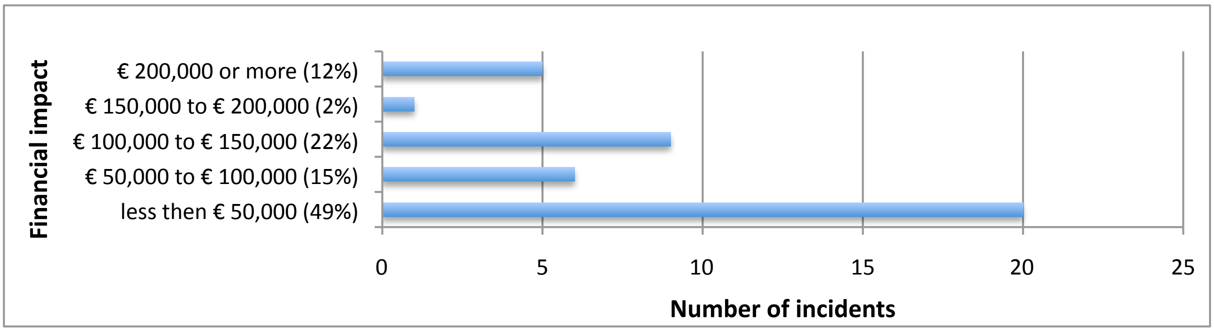
The first dimension is the technical impact of incidents. The reported incidents are classified into five categories based on their intensity on the technical performance of Oxilion's services, namely: (1) incidents that were potentially dangerous but had at that time no impact, (2) incidents that limited the ability to administer services but had no direct impact on customers, (3) incidents that reduced the performance of services (e.g. slowdown), but didn't totally disable them, (4) incidents that caused some function of a service to fail, but did not disable the service as a whole and (5) incidents that caused complete unavailability (downtime). Figure 8 provides an overview of the number of incidents in each category. The categories are ordered sequentially: a risk being the least distressing type of incident and downtime the most distressing type of incident.

Figure 8: number of reported incidents categorized according to the intensity of technical impact



The second dimension is the financial impact of incidents, meaning: the total sum of annual turnover at risk during an incident. Annual turnover at risk is the turnover (in euro's per year) generated by products and services installed on or executed by the system(s) involved in an incident. Hence: with each incident the study posed the question: how much annual turnover would the company miss if all services used by the affected system were terminated due to the incident? The answer to this question was calculated by multiplying the number of customers that used the impacted system with the average annual turnover they generated (with that specific system)[8]. Figure 9 provides an overview of the potential financial damage of the incidents that occurred during the study.

Figure 9: number of reported incidents categorized according the magnitude of financial impact



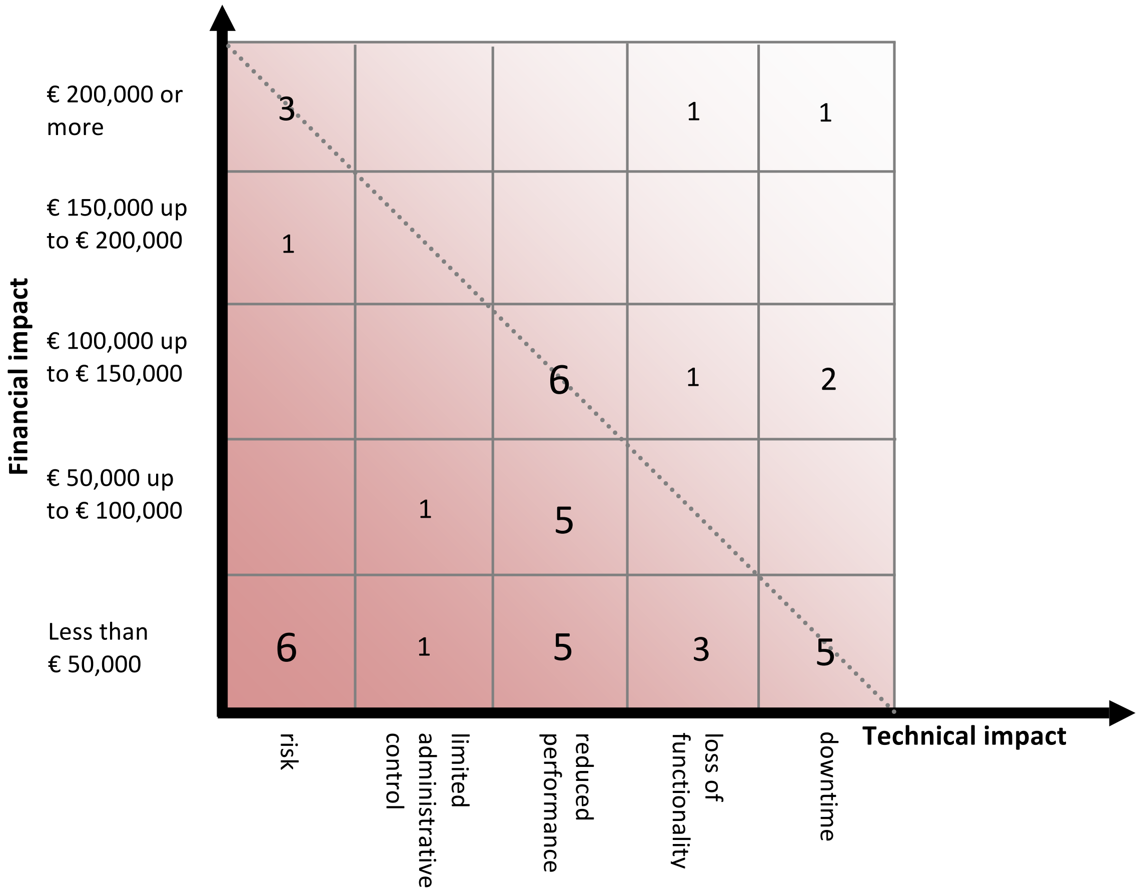
One can deduce from figure 9 that incidents can have a significant impact on business if managed inappropriately. To put the potential damage of incidents into perspective: € 50,000 annual turnover (the lowest category) translates to roughly 2.5% of the total annual turnover of Oxilion. This implies that with inappropriately managing a single incident of the highest category, Oxilion could lose 10% of its annual turnover. Additionally, if all incidents were managed inappropriately Oxilion could lose more than one and a half times its annual turnover (the sum of the financial impact of al incidents, based on the average of each category times the number of incidents in the respective category is € 3,250,000).

Note that in reality none of the incidents caused any monetary damage. This can be taken as a sign that Oxilion acted appropriately as perceived by their customers. The company was thus able to meet the promised performance level (even tough Oxilion's performance level suffered some damage). However, the interviewees expressed that, had the company acted inappropriately, these incidents might have escalated and might have resulted in real monetary damage.

[8] The researcher of this study is well aware that this is a crude measurement scale. However, it would have been very time-consuming to calculate the exact potential damage of a single incident given that it is contingent on numerous factors. Moreover, calculating the exact potential damage of each incident would not have contributed to the aim of this part of the study (namely: to describe individual's motivation and knowledge). A simple and crude measurement scale therefore serves the purpose of providing a general 'picture'.

Figure 10 depicts the technical impact of incidents and financial impact of incidents plotted in one matrix. Incidents that are placed in the lower left corner of the matrix represent incidents with relative low potential impact, while incidents that are placed in the upper right corner of the matrix represents incidents with relative high potential impact. The dotted line signals the transition from low to high potential impact. The incidents that are situated on or above the dotted line are the kind of incidents that should be avoided at all times. One can thus deduce that almost half of the incidents had a high potential impact while over half of the incidents had a low potential impact.

Figure 10: number of incidents and their impact described along two dimensions



	risk	limited administrative control	reduced performance	loss of functionality	downtime
€ 200,000 or more	3			1	1
€ 150,000 up to € 200,000	1				
€ 100,000 up to € 150,000			6	1	2
€ 50,000 up to € 100,000		1	5		
Less than € 50,000	6	1	5	3	5

The matrix (figure 10) suggests that the impact of incidents (technical and financial) varies per incident. This variation can be explained by the fact that (apart from seven spam runs) every incident was unique, meaning: almost every incident posed a new problem that was not encountered before. However at a higher level of analysis one can see a pattern (Appendix C). Based on the cause of the incidents one can conclude that most incidents related to a software failure. Hardware failures were relatively sparse. The Financial Director commented on this observation as following:

> "Software is an element of our product where, compared to other elements, a lot of things can go wrong. You just buy hardware and it works. Software however cannot be bought with a guarantee that it will work out of the box. Moreover, if software works properly there is always a chance that it will break down due to customers who are installing hacks or bad scripts"

From the quote of the Financial Director one can deduce that hardware is a relatively 'static' element, whereas software is a relatively 'variable' element of hosting. Hardware can only be altered by the provider and is placed in a protected environment, while software can be altered by the customer and is prone to external forces (e.g. upgrades, bugs, hacks). One can also interpret this difference alternatively and argue that software failures are actually people failures (e.g. people install incompatible software). The analysis reveals that if software failures are conceptualized in this way (Appendix C), customers, employees and manufacturers are each responsible for 31%, 38% and 31% of failures related to software respectively.

Until now only two dimensions were discussed to measure the impact of incidents, namely the technical impact and the financial impact of incidents. In their logbooks employees put forth a third dimension: the perceptual impact of incidents. An incident can influence public perception about a provider. Generally, employees are aware of this dimension of potential impact. For example, in reaction to a large incident an employee wrote:

> "There are a dozen valid technical reasons why our service did not work properly. It should however work! We are known for being highly reliable. The incident has badly damaged our reputation."

The employee proofed to be right: the incident resulted in negative media coverage and complaining customers. Based on the times that a specific dimension of impact was named in the diary entries, one can conclude that employees are better in estimating the technical and perceptual impact of incidents than the financial impact of incidents. However, note that employees were always able to estimate the impact of incidents in minimally one dimension. This awareness helped employees to judge what action was appropriate.

4.2 BEHAVIOUR

The previous section described the impact of incidents on the reliability level of a hosting provider. This section provides some insights into behaviour that employees showed to manage these incidents. As mentioned in the theoretical framework, behaviour is defined as "any denotable overt action that an individual, a group of individuals, or some living system performs" (Jaccard & Blanton, 2005, p. 131). Behaviour can be split into four elements: "(1) an action, (2) an object or target toward which the action is directed, (3) a setting and (4) a time" (Jaccard & Blanton, 2005, p. 131). Only the first two elements were acknowledged to be relevant for this study. In total 83 different combinations of actions and objects or entities were observed. The combinations encompassed 25 different actions and 16 objects or entities.

In order to analyse employee's behaviour two classifications were used: a classification based on the Information Technology Infrastructure Library (ITIL) V3 Incident Management and a classification based on the object or entity towards which action was directed. Figure 11 depicts the classification based on ITIL (for more information see Appendix D). The classification was slightly adapted to fit the processes in Oxilion and to provide a more comprehensive overall 'picture'.

Figure 11: categorisation of behaviour based on ITIL V3 incident man. (adopted from Van Bon, 2008)

A - Incident detection and recording
Incidents are detected and reported by customer or monitoring tool.

B - Classification and initial support (15%)
Incidents are generally classified and assigned to employees by 1^e line support.

Behaviour: prioritizing tasks, informing colleague, coordinating tasks, warning colleague.

C - Investigation and diagnosis (24%)
Incidents are investigated and diagnosed by 1^e line support or 2^{nd} line support (engineers).

Behaviour: searching logs, calling helpdesk, suspending user account, consulting colleague, searching solution, turning off service, turning off monitoring tool, checking monitoring tool, searching script, checking power supply

D - Resolution and recovery (61%)
Solutions are implemented by 1^e line support or 2^{nd} line support (engineers)

Behaviour: configuring server, rebooting server, modifying network, clearing server, deleting user account, restoring software, upgrading software, deleting IP's, rebooting virtual server, replugging server, removing script, restoring files, migrating virtual server, checking load, removing files, clearing mail queue, restarting service, calling service desk, installing hard disk, isolating server

E - Incident closure
Incidents are reported as closed by the employee who handled the incident.

Comment: percentages represent the number of times behaviour in the respective ITIL category was described in employee's diaries (Appendix D).

From figure 11 one can deduce that two third of employee's behaviour was aimed at resolution and recovery of incidents. Hence, this behaviour was aimed at implementing a solution. Approximately a quarter of employee's behaviour was aimed at investigating and diagnosing incidents. A minority (15%) of employee's behaviour was aimed at classification of incidents and offering initial support. Employees did not describe any behaviour that can be categorized in the first and fifth category. Behaviour aimed at incident detection (first category) was naturally not described given that this task is generally carried out by customers or monitoring tools. Employees did also not describe their behaviour regarding recording and closing incidents. This behaviour was probably not described since these are relative trivial actions (from an employee's point of view).

In addition to the observations stated above, one can observe that the number of different behaviours varies per category. The data suggests that resolution and recovery of incidents requires relatively varied behaviour. Investigating and diagnosing incidents requires less varied behaviour whereas classification of incidents and offering initial support requires relatively little varied behaviour. Although overall employee's behaviour is divers, one could thus conclude that there is varied diversity in behaviour depending on the phase of the incident.

The second classification used in this study is based on the object or entity to which action was directed (for more information see Appendix D). Based on this classification, behaviour can be categorized into four different categories, namely: (1) behaviour aimed at software, (2) behaviour aimed at hardware, (3) behaviour aimed at administrative objects and (4) behaviour aimed at people. This classification demonstrated that most actions (49%) are directed towards software. These actions were either aimed at searching for a problem (e.g. checking monitoring tool) or at implementing a solution (e.g. upgrading or restarting services). The actions directed towards software did typically entail multiple small actions that were interconnected and interrelated. Hence, behaviour aimed at software is in general more complicated than behaviour directed towards other objects or entities.

The second largest category of employee's behaviour was behaviour directed towards hardware (22%). These actions were generally aimed at reviving hardware (e.g. rebooting a server). Contrary to the actions in the software category, this category included relatively simple actions (e.g. so to speak 'pushing a button'). Administrative actions (15%) were generally aimed at changing a customer's status while actions aimed at people (14%) typically involved interacting with internal or external contacts.

4.3 MOTIVATION

As explained in the theoretical framework, behaviour is guided by an individual's motivations. Motivation was defined as "the individual's intention to perform a given behaviour" (Ajzen, 1991, p. 181). The theoretical framework explained that an individual's motivation is the function of an individual's attitude (an evaluative disposition) and subjective norms (perceived social pressure).

The theoretical framework classified motivations into two categories of motivations: motivations aimed at anticipating to threats and motivations aimed at containing the effects of threats that had occurred. The survey assessed the level of both forms of motivations. Employees were asked to rate their agreement with statements that represented specific motivations (on a scale from 1 to 5). The higher they rated a specific statement, the more they possessed a specific motivation. Given that the survey was based on Weick & Sutcliffe's (2007) audits, their threshold was used to put the scores into perspective. The authors defined a threshold of 3.3 for both categories of motivations. Hence, they consider organizations that score a 3.3 or higher to be organizations that possess appropriate motivations.

On average Oxilion scored a 3.9 on motivations aimed at anticipating threats and a 4.2 on motivations aimed at containing threats. Figure 12 depicts the score of both categories of motivations as perceived by each employee. Note that two employees (nr. 5 and nr. 10) score a 3.3 or lower on motivations aimed at anticipating. These employees thus perceive that the organization is moderately good at anticipating.

Figure 12: overview of the level of motivations aimed at anticipating and containing threats

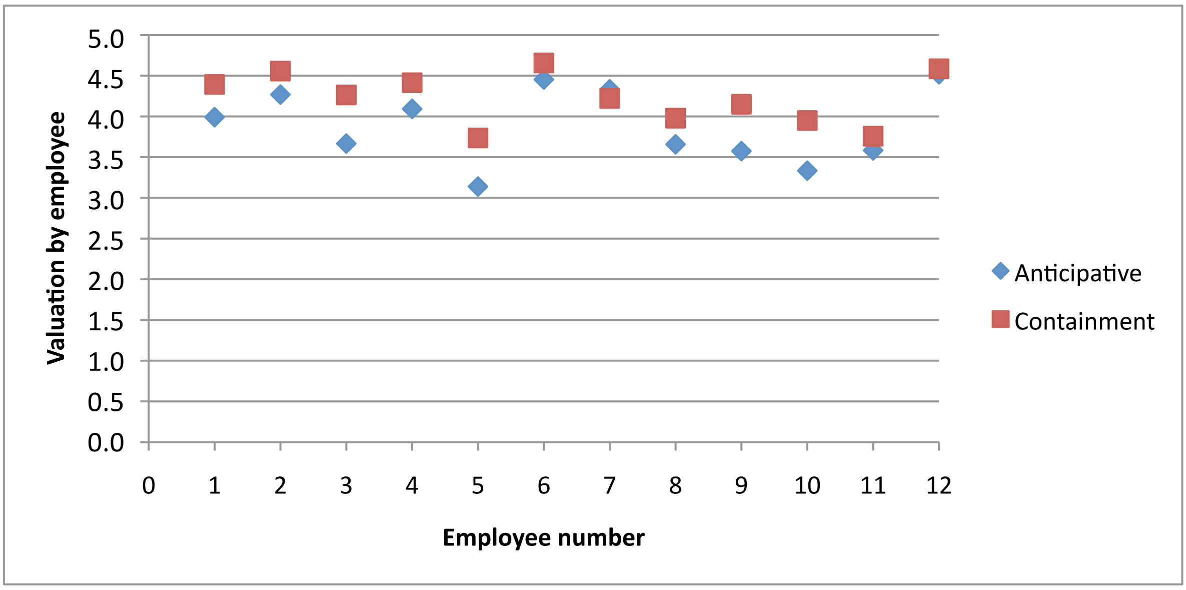


Figure 12 reveals a pattern: generally motivations aimed at containing threats are rated higher than motivations aimed at anticipating to threats (apart from employee nr. 7). Hence, employees perceive that they are better in containing threats than anticipating to threats. In an interview with the Financial Director it becomes clear why this is the case:

> "It is difficult to define all possible scenario's in which something can go wrong in advance. There are things that you just cannot anticipate to. Something unexpected happens only once. The next time the same incident takes place it is discovered by our monitoring tools and taken care of by our staff."

The quote from the Financial Director clarifies that all possible interactions of Oxilion's complex and changing technology cannot be understood and anticipated to in advance (when their infrastructure is developed). Employees are therefore often ‘trouble-shooting’ (during daily operations), meaning that they are containing the effects of incidents that have already occurred. As a consequence, employee’s motivations are more directed at containing threats than anticipating to them. In short, employee’s motivations are thus focused on containment given that these motivations guide employees to show appropriate behaviour to eliminate threats to reliability. Three classes of motivations demonstrated to be especially important for containing threats (Appendix F), namely: motivations regarding diagnosis and resolution, motivations regarding communication and collaboration, and motivations regarding knowledge development and sharing. These classes of motivations stood out above the rest because they were frequently referred to in the diaries or were rated highly in the survey.

The first class of motivations found to be especially important for containing threats are employee’s motivations regarding incident diagnosis and resolution. The motivations in this class entail mainly injunctive norms, meaning: perceived social pressure from Oxilion’s customers and management to show specific behaviour because it is typically approved of. These norms guide how an employee should handle incident diagnosis and resolution. The norm during diagnosis is that employees should react to incidents quickly, inquire the issue at hand and limit further damage. If the diagnosis stage takes longer than expected, employees should provide updates of the incident’s status. The norm during the resolution phase is that solutions should not be quick fixes. Instead it is regarded as important that a permanent solution is found. In addition it is regarded as important that employees double-check the diagnosis and the resolution of an incident.

The injunctive norms stated above are maintained by communication. In other words: employees know what is and what is not approved of by verbal (e.g. customer complaints, informal rules as expressed by the management) and nonverbal communication (e.g. setting an example). The next quote is a good example of how these injunctive norms were formed. This quote refers to the injunctive norm of finding a permanent solution.

> “I tell my employees that if a server is down they must get it up and running quickly. However, if they can figure out a permanent solution to the problem they are allowed more time (to some extent). The server may be down longer, but the problem won’t occur again.”

In addition to the injunctive norms stated above one descriptive norm was observed. This norm related to incidents that occurred on systems that were scheduled for an update. If this happened the descriptive norm was that instead of diagnosing the incident, the system should just be updated since it would likely solve the problem. This norm guides thus behaviour by providing confirmation as to what is likely effective.

Furthermore, an innovative attitude was found to be important to facilitate the diagnoses and resolution of novel incidents. Given that most incidents were unique, meaning that almost every incident posed a new problem that was not encountered before, it was regarded as important that employees held a positive attitude towards developing new and creative ideas. This enabled employees to manage novel incidents and come up with new solutions.

The second class of motivations found to be especially important for containing threats are employee's motivations regarding communication and collaboration. The diary entries and the survey results revealed that employees (particularly engineers) hold a positive attitude towards questioning and discussion. The Technical Manager describes this attitude as "inquisitive":

> "Engineers are typically very inquisitive. Moreover, they like to bring forth their view on issues. Therefore people are always willing to assist a colleague with a problem and are happy to discuss an issue. Maybe it is not the most productive way to work, but it does help to understand and solve problems."

Attitude is however not the only factor that influences employee's motivations regarding communication and collaboration. Oxilion has established some injunctive norms that facilitate communication and collaboration. The company nourishes a culture of commitment and mutual respect in which questioning is encouraged and in which people feel free to talk about problems to colleagues or superiors. The Technical Manager expressed this as following:

> "We [the management of Oxilion] are stimulating open communication. The last thing we want is creating separate departments. We are stimulating this by setting an example, working together with employees and meeting with all employees on weekly basis. This keeps everybody on the same page and it stimulates involvement from all employees since everybody knows what is going on in the organization."

In short, employee's motivations regarding communication and collaboration are a combination of employee's attitudes and injunctive norms. These motivations bring forth a willingness to help others, commitment, respect, questioning and discussion. This enables employees (as a group) to cover a broader range of possible causes for incidents and come up with better solutions.

The third class of motivations found to be especially important for containing threats are employee's motivations regarding knowledge development and sharing. The diary entries and the survey results revealed that employee's (particularly engineers) hold a positive attitude towards acquiring and sharing knowledge. Employees frequently expressed that they could and should learn from the problem that they had just solved. Moreover, they also expressed that their colleagues could learn from the incident as well. The quote below provides an example of this attitude:

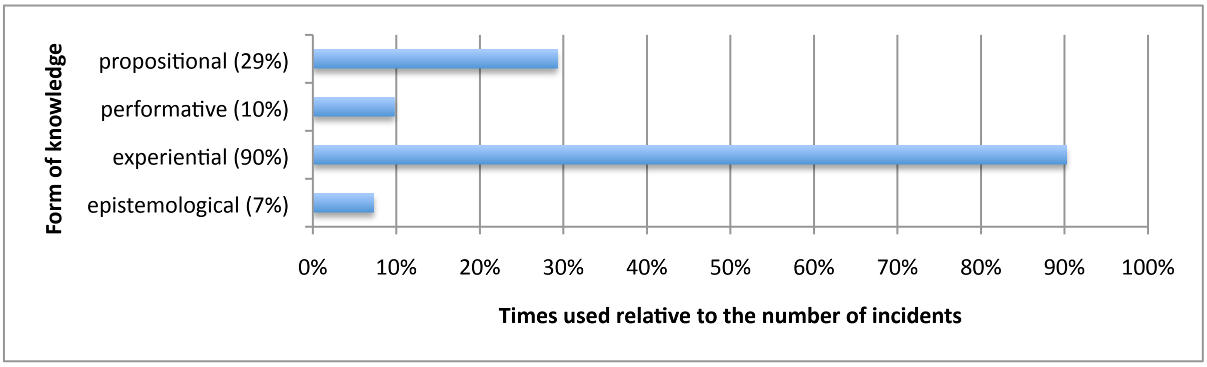
> "I got the instructions from Engineer A, so that next time I can handle problems like this myself. I stored the instructions in my own knowledge database. When I have got enough information I write a 'manual' and publish it on the company's internal wiki."

The quote above clarifies that employees consider it important to learn from mistakes since they think that the knowledge acquired during previous incidents could proof to be valuable during upcoming incidents. This positive motivation towards knowledge development and sharing was partially[9] enforced by injunctive norms.

4.4 KNOWLEDGE

This section provides some insights into employee's knowledge. In the theoretical framework knowledge was defined as: "a capability with the potential for influencing future action" (Alavi & Leidner, 2001, p. 111). Knowledge specifies potential behaviour an employee is capable to show. The theoretical framework described four forms of knowledge adopted from Mingers (2008): propositional knowledge (to know that x), performative (to know how to do x), experiential (to know x) and epistemological (to know why x). The qualitative research diary method was used to assess what forms of knowledge were used in order to manage threats. Figure 13 provides an overview of the times a form of knowledge was used relative to the number of reported incidents. Note that multiple forms of knowledge can be used during one incident. Also note that figure 13 only depicts propositional knowledge that was used during the incident, not the propositional knowledge described in incidents notifications provided by monitoring tools or customers[10].

Figure 13: overview of the forms of knowledge used to manage threats



From figure 13 one can deduce that experiential knowledge is (by far) the major type of knowledge used to manage threats to reliability. Mingers (2008) describes that the 'depth' of experiential

[9] The researcher observed these injunctive norms, but contrary to other norms were they less emphasized by organizational members and not expressed by all members of the organization.

[10] Incident notifications sent by customers or monitoring tools were not included in the analysis. Had the study included this information (propositional knowledge) in the analyses, propositional knowledge would score a 100% given that every incident contains initially information.

knowledge can be very variable. Based on the depth of the knowledge concerned, this study distinguishes between two levels: experiential knowledge used to contact people and experiential knowledge used to solve problems. The first level of experiential knowledge signals an acquaintance with an entity, while the latter level of experiential knowledge signals that an individual has a complex set of understandings about an object or entity.

The first level of experiential knowledge was used when an employee had to get in contact with somebody to discuss an issue. Often this meant interacting with colleagues. Note that the employee knew from personal experiences whom to contact. Hence, they knew that a specific colleague could probably help them because they were acquainted with the colleague concerned.

The second level of experiential knowledge has more ‘depth’ than the first level. Employees described this level of experiential knowledge as: “learning-by-doing”, “self-taught knowledge” and “experience”. The employees meant that they had a complex set of understandings and experiences about specific software. The Financial Director explained the frequent use of this level of experiential knowledge as following:

> “Our industry is characterized by ‘experience’. This kind of knowledge is an absolute necessity. There can be, so to speak, four or five hundred different causes or a combination of causes for a single incident. Only a experienced employee can deduce from often multiple and mixed signals what the cause is of an incident.”

From the quote above, one can infer that the relative high use of experiential knowledge originates from operating complex and changing technology. The technology used by Oxilion is either too specific or too much the subject of change to be learned in nearly all types of formal education. An employee must be very experienced in a specific technology for him to be able to interpret signals of a failure correctly and implement a solution.

The second most used form of knowledge was propositional knowledge. Propositional knowledge was information acquired or sent by employees to enable the diagnoses and resolution of incidents. Most of the time it entailed acquired information from a colleague.

The third most used form of knowledge was performative knowledge. This type of knowledge was used to solve incidents related hardware. It meant that the employee possessed a certain skill or competence to handle specific hardware (e.g. install a server correctly). Given that the limited number of hardware failures, performative knowledge was not much used by employees.

The least used form of knowledge was epistemological knowledge. Occasionally employees said that they learned how to do something in a course provided by a manufacturer. Employees were thus referring to epistemological knowledge. They had a deeper understanding of specific technology due to formal methods learned in a course. Employees never revered to any formal education such as a bachelor or a master degree. As previously said, Oxilion's technology is either too specific or too much the subject of change to be learned in nearly all types of formal education.

The fact that epistemological knowledge was used relatively little should be taken as a sign that epistemological knowledge is not important for eliminating threats to reliability. However, the interviewees pointed out that a person's acquired epistemological knowledge might be a good indicator for an individual's learning capabilities.

5 MONITORING AND LEARNING

This chapter describes the underlying logic of the monitoring and learning tool (M&L-tool) and explains how it can facilitate both monitoring and learning. The chapter is structured along the lines of the main variables of this study as described in the theoretical framework (reliability, behaviour, motivation and knowledge). Each section describes one part of the tool.

5.1 RELIABILITY

The previous chapter showed that incidents could threaten the reliability of Oxilion's infrastructure. It also established that incidents could have significant impact on business if managed inappropriately. Additionally, the previous chapter demonstrated that acquiring and storing information about incidents could assist the organization in achieving high reliability in two ways: (1) information about the (potential) impact of single incidents can help employees judge what action is appropriate and (2) information about the (potential) impact of multiple incidents can be used to determine the over-all reliability level of the organization. In addition, the previous chapter demonstrated that information (propositional knowledge) acquired during previous incidents could be valuable for upcoming incidents. This implies that acquiring more and more information about previous incidents enables employees to cover a growing range of incidents. It enables them to contain the effects of incidents better and faster. This stresses the importance of effective knowledge sharing and storing systems to aid learning. Based on these findings one can drawn several requirements for the M&L-tool:

> *Requirement 1:* The tool should present real-time information about the financial impact of single incidents to facilitate an appropriate reaction.
>
> *Requirement 2:* The tool should provide a periodic overview of the number and impact of incidents, and consequently of the reliability level of Oxilion.
>
> *Requirement 3:* Employees should be able to register and retrieve detailed information about incidents (e.g. signals of failure, causes and solutions) to aid knowledge storing and sharing.

This study proposes that Oxilion implements an incident database. The proposed database is in principle a digital archive that employees can use to store information about incidents and retrieve information about previous incidents. It functions similar to the diary collection method used in this study, meaning that it encompasses reporting and analysing incidents. However, contrary to the diary collection method, the incident database analyses incidents automatically[11]. The design of the database (database structure) is described in Appendix G.

Figure 14 illustrates the digital form used to report incidents and store its information in the database. Employees need to fill out this digital form if they encounter an incident. The form consists of multiple items. However, due to high degree of automation only information about the technical impact of an incident, information about the diagnosis and resolution of an incident, and information about the cause of an incident needs to be filled out. Other information (time, employee name and financial impact) is registered automatically. Hence, the amount of information employees need to fill out is limited. This saves time. Note that the form also depicts the potential impact of incidents. Given the link with the database of the financial administration this information can be depicted in real-time (Requirement 1).

Figure 14: Digital form for reporting incidents (mock-up)

Report an incident			
Data:	12-06-2010	Technical impact*:	Reduced performance (dropdown menu)
Reported by:	Employee X	Financial impact:	€ 6,000 (p/m)
System:	Server 125	Customer(s):	Customer X
Cause*	Plesk (dropdown menu)		
Diagnosis & Resolution*	(Text input)		

Comment: items denoted with a * need to be filled out manually.

The information in the incident database can be used to provide an overview of the reliability level of Oxilion (Requirement 2). Each month the M&L-tool generates a report of the reliability level of the company. A mock-up of the report can be found in Appendix H. With this report Oxilion has an overview of the technical and financial impact of incidents, and how this compares to previous months. Additionally, the report describes which technology is relatively often the source of incidents and has thus a high risk factor (input for engineers). Furthermore, the report describes which customers are relatively often involved in incidents and might therefore be dissatisfied (input for sales consultants).

[11] Note that the way in which data is gathered with the M&L-tool differs from the way data was gathered in this study. In the study data was gathered and analyzed by hand. The database could automatically gather and analyse data due to a link with other databases, such as the database of 'server registration' and the financial administration. Additionally, in this study the approximate potential financial impact of incidents was calculated by hand. The tool should calculate the potential financial impact of incidents automatically and more accurately by adding up the exact (annual) turnover of all customers involved in the incident.

The incident database could also fulfil the third requirement by providing a tool that facilitates organizational learning or, to be more specific: single-loop, double-loop and deutero learning. Single-loop learning entails recognizing a problem and selecting an appropriate mode of solving it from an existing base of modes (Wijnhoven, 2001) similar to the routine of a thermostat (Beeby & Booth, 2000). The single-loop learning cycle in the context of this study includes four (simplified) steps. It starts with the notion that 'something' is out of the ordinary and consequently an incident is reported (step 1). The incident is diagnosed (step 2) during which it is recognized as incident that has occurred before. Given that the incident is not new, an existing appropriate strategy to manage the incident is selected from the incident database (step 3) and the incident is resolved (step 4). Note that in the context of this study, single-loop learning would only occur sporadically. The study showed that most incidents were unique (see page 34). Hence, they were never encountered before. An existing strategy to manage these incidents would therefore not be available. One would thus need to develop new strategies. This calls for double-loop learning. Double-loop learning entails developing new modes to cope with a problem because existing modes are ineffective (Wijnhoven, 2001). Unlike single-loop learning, which is routine (Beeby & Booth, 2000), double-loop learning is non-routine. Moreover, Wijnhoven (2001) links double-loop learning to innovation. The double-loop learning cycle starts with the discovery of an incident (step 1). In the diagnoses stage (step 2), the incident is diagnosed and recognized as an incident that has not occurred before. Existing strategies would thus be ineffective. Therefore, the organization needs to innovate and assess their current database of strategies (step 3). Existing strategies may need to be altered or combined to develop a new strategy (step 4) and resolve the incident (step 5)

Note that the incident database is used in both learning loops. During the single-loop the database is used to select an existing strategy (which is retrieved from the database), whereas during the double-loop the database is used to form a new strategy (by combining existing strategies and store a new strategy in the database). The more the company passes trough double-loops, the more strategies are stored in the database. Hence, the more the company learns, the more incidents it is able to cover.

As time progresses the incident database of the M&L-tool contains more and more information (strategies, causes of incident et cetera). If analysed this information can be used to create an overview of incidents (such as in appendix H). Given Oxilion's rapid changing environment this overview is prone to changes. It might surface new developments and these new insights might lead to discussions about the nature of the M&L-tool. The organization might ask itself which type of incidents it copes with efficiently and which type not (and why not). This might in turn result in an adjustment in the way the organization learns. Hence, the organization might discover that the current way of learning needs to change due to its changing environment. The adjustment of the current learning style to changing environmental learning needs is called deutero learning (Wijnhoven, 2001)[12]. It is reflexivity about learning itself: "learning to learn" (Freeman, 2007, p. 478). Note that the adoption of the M&L-tool in itself is also deutero learning since it also involves learning a new way to learn.

In short, the M&L-tool as described above could facilitate systematic storing of all kinds of information about incidents. This information can be used to monitor reliability on the level of a single entity (e.g. a server) but also on an aggregated level (e.g. the whole company). Additionally, the tool could contribute to single- double- and deutero learning within the organization. With each incident added to the database of the M&L-tool, more information is available that could help employees trace causes of incidents faster and find solutions more rapidly by combining knowledge acquired during previous incidents. Over time this information might lead to new insights that in turn might lead to an adjustment of the organization's learning style.

5.2 BEHAVIOUR

The previous chapter described that in order to cope with incidents employees need to show all kinds of behaviour. Behaviour is highly contextual, meaning that it is dependent on the incident in question. This implies that a tool to monitor behaviour should encompass a wide range of behaviours. In addition, the previous chapter described that most incidents were unique. They were not encountered before and therefore required a new combination of actions. This implies that it is impossible to determine in advance what behaviour is appropriate to cope with incidents. It would thus require someone who afterwards (manually) determines whether showed behaviour was appropriate.

The highly contextual nature of incidents and the fact that behaviour can only be checked post facto poses some practical difficulties. It implies that monitoring behaviour cannot be automated and therefore that it would be very time-consuming to determine whether specific behaviour was appropriate. For that reason, this study proposes that behaviour is not monitored[13]. This does not have far reaching consequences. Behaviour is positioned amid the other variables. The M&L-tool monitors the variables prior to behaviour (motivation and knowledge) and the variable succeeding behaviour (reliability). Hence, behaviour is thus monitored indirectly via the other variables.

[12] Note that deutero learning has different conceptualizations. Some authors call it meta-learning (Visser 2007).

[13] An alternative to not monitoring behaviour would be to monitor behaviour (periodically) similar to the diary collection method. Employees would be required to describe their actions or an authority (e.g. manager) would need to observe employee's actions. Subsequently, an authority would need to determine whether these actions were appropriate. However, this type of monitoring would require excessive investment of employee's time.

5.3 MOTIVATION

The previous chapter described that all possible interactions of Oxilion's complex and changing technology cannot be understood and anticipated to in advance. Therefore, employees are often 'trouble-shooting', meaning that they are containing the effects of incidents that have already occurred. This stresses the importance of containment motivations. This study demonstrated that three classes of motivations are especially important for containing the effects of incidents effectively, namely: (1) motivations regarding diagnosis and resolution, (2) motivations regarding communication and collaboration, and (3) motivations regarding knowledge development and sharing. Based on these findings one can draw two requirements for a tool to monitor motivation:

> *Requirement 1:* The tool should focus on monitoring containment motivations given these motivations are needed to guide appropriate behaviour needed during 'trouble-shooting'.
>
> *Requirement 2*: The tool should especially monitor the three classes of motivations that are important for containing the effects of incidents effectively.

This study proposes that Oxilion conducts a half-yearly internal survey to monitor employee's motivations. A mock-up of the survey can be found in Appendix I. The survey consists out of 25 statements. Each set of five statements addresses a topic that is important for realizing reliability. The first and second set of statements test whether employees possess appropriate anticipative and containment motivations (requirement 1). The other sets are more specific. They focus on the motivations that are especially important for eliminating threats to reliability, namely: motivations regarding diagnosis and resolution, motivations regarding communication and collaboration, and motivations regarding knowledge development and sharing (requirement 2).

The survey uses a five-point Likert scale (1 = totally disagree and 5 = totally agree); the higher the score, the better employee's attitude. An item that scores a 3 or lower should be considered as worrying. Hence, these specific motivations should thus be stimulated. Oxilion might be inclined to conduct the survey among technical employees only, given that these employees influence reliability directly. However, it is good to include the view of other employees since this will provide a more balanced 'picture'. All employees should thus be included in the survey sample. The best form to conduct the survey is an anonymous self-administered survey so that employees are stimulated to answer open and honestly. Moreover, it is likely that this has a positive affect on the return rate. To further improve the return rate Oxilion should sent reminders to employees that have not yet filled in the survey after the (first) deadline. A return rate close to a 100% is preferable.

5.4 KNOWLEDGE

The previous chapter described that experiential knowledge is (compared to other forms of knowledge) by far the major type of knowledge used to mange threats to reliability. This form of knowledge was needed nine out of ten times to cope with incidents. The previous chapter demonstrated that employees need, what this study calls, the second level of experiential knowledge in order diagnose and resolve incidents effectively. This form of knowledge entails a complex set of understandings about specific software. Based on these findings one can draw the following requirement:

> *Requirement 1:* The tool should focus on monitoring experiential knowledge, especially the second level of experiential knowledge (a complex set of understandings about specific software).

The characteristics of experiential knowledge impose some limitations on the design of the monitoring tool, namely: (1) experiential knowledge is embodied and (2) the source of experiential knowledge is personal experience (Mingers, 2008). This implies that experiential knowledge is difficult to monitor and that it is likely depending on a subjective assessment. Therefore, this study proposes that Oxilion conducts a half-yearly assessment to monitor experiential knowledge.

Figure 14 (on the next page) depicts the assessment tool. The assessment consists of a number of items; each item focuses on experiential knowledge related to specific software. Note that this software is highly provider and time depended. It encompasses software that is currently used by Oxilion or software that will be used by the company in the near future. An authority (e.g. technical manager) should assess the level of experiential knowledge of each employee. The authority should be in the position to make a good assessment. Hence, he or she should have a good understanding of someone's capabilities.

The assessment tool uses two measurement scales, namely: (1) a scale to measure whether employees possess particular experiential knowledge and (2) a scale to measure whether employees have to increase their experiential knowledge. Two scales are used because a low score on the first scale does not automatically imply that an improvement is needed. Oxilion might for example have decided that only one expert in particular software is needed. The other employees would therefore not have to improve their experiential knowledge. Hence, the first scale is used to map the current level of experiential knowledge while the second scale illustrates what would be the desired score.

Figure 14: Form to assess experiential knowledge

	VMware		**Linux OS**		**Windows OS**		**PHP/MySQL**		**Direct Admin**		**Plesk**	
	Cur.	Des.	Cur.	Des.	Cur.	Des.	Cur.	Des.	Cur.	Des.	Cur.	Des.
Employee 1	++	=	++	=	-	=	++	=	+	>	++	=
Employee 2	-	=	++	=	-	=	++	=	++	=	--	=
Employee 3	+	>	+	=	-	=	+	>	+	>	+	=
Employee 4	--	=	+	=	++	=	+	=	-	-	++	=
Back-up?	P	Y	Y	Y	N	N	Y	Y	P	Y	Y	N

↑ **Description:** The measurement scale of the current level of experiential knowledge is a five-point scale, ranging from: -- (denoting strongly insufficient) to ++ (very good). The measurement scale of the desired level of experiential knowledge is three-point scale, ranging from: = (denoting no improvement need) too >> (improvement strongly needed). The last row describes whether there is currently somebody who can function as back up for a specific technology and whether the organization desires whether somebody can function as a back up. N = no, P = partially, Y = yes.

6 CONCLUSIONS

This chapter provides an answer to the research questions and discusses their implications. In addition, the study's limitations are discussed followed by its contributions to practice and theory. At the end of the chapter several suggestions for future research are described.

6.1 CONCLUSION

The study established that the major consequences of a slow-or breakdown pressure Oxilion to achieve a flawless performance. It needs to be highly reliable while coping with threats originating from its complex and changing technology. These threats, in the form of incidents, can have significant impact on business when managed inappropriately. Therefore, Oxilion's employees need to take appropriate action if incidents occur. Their behaviour is guided by their motivation and specified by their knowledge. However, Oxilion does not know what motivation and knowledge employees must posses in order to show appropriate behaviour. Consequently, the first research questions is:

> *RQ 1:* What motivation and knowledge is needed to create appropriate behaviour that enables reliability?

Oxilion cannot understand all possible interactions of its complex and changing technology in advance. The organization is therefore unable to anticipate to all possible interactions during the design of its infrastructure. This organizational characteristic largely influences the way in which employee's motivation and knowledge are configured.

First of all, given the limited understanding of all possible interactions, anticipative motivations can only help the organization realize reliability to some degree. Anticipative motivations can only be deployed during the design of Oxilion's infrastructure. During daily operations employees are often 'trouble-shooting', meaning that they are containing the effects of incidents that were not anticipated during the design of the company's infrastructure. This stresses the importance of containment motivations. Three classes of motivations proofed to be especially important for containing the effects of incidents effectively, namely (1) motivations regarding diagnosis and resolution, (2) motivations regarding communication and collaboration, and (3) motivations regarding knowledge development and sharing. The first class of motivations encompasses five injunctive norms: (1) inquire issues, (2) react quickly, (3) limit further damage, (4) inform the customer timely, (5) double-check and (6) implement permanent solutions. The first class encompasses one descriptive norm: (7) if an incident occurs on a system that is scheduled for an update, the system should be updated instead of starting a diagnosis of the incident. Additionally, the study demonstrated that one attitude is important for diagnosing and resolving (often novel) incidents, namely: (8) an innovative attitude. The second class of motivations (communication and collaboration) is a mix of two attitudes and three injunctive norms that all enable communication and collaboration. Employees should hold a positive attitude towards (1) questioning and (2) discussion. Additionally, communication and collaboration is enforced by three injunctive norms: (3) respect colleagues, (4) be committed and (5) help others. The third class of motivations encompasses mainly attitudes, namely a holding positive attitude towards (1) knowledge development and (2) knowledge sharing. These attitudes were partially enforced by injunctive norms.

Second, given the limited ability to understand all possible interactions of Oxilion's complex and changing technology in advance, and consequently the focus on containment, employees need mainly experiential knowledge. This knowledge enables them to interpreted signals of a failure correctly and implement solutions effectively. Only experienced employees can deduce from often multiple and mixed signals what the cause was of an incident. This form of knowledge, in this study called the second level of experiential knowledge, was needed to solve seven out of ten incidents. It entailed a complex set of understandings about specific software that enabled diagnosis and resolution of incidents. However, in some cases, employees were unable to diagnose or solve incidents themselves. They were therefore required to contact somebody who could help them. This study named this form of knowledge the first form of experiential knowledge. It was needed to facilitate effective interaction between colleagues. This form of knowledge entails a set of personal experiences regarding entities, used to contact the right entity and acquire information that facilitates the diagnoses and resolution of incidents. The first level of experiential knowledge was needed to solve three out of ten incidents.

In order to realize high reliability, Oxilion should not only be able to create appropriate motivation and knowledge (an thereby behaviour and reliability), the organization should also be able to monitor any changes in these variables. Therefore, the second research questions is:

RQ 2: How should motivation, knowledge, behaviour and reliability be monitored?

In order to realize reliability, Oxilion should use a monitoring tool that consists out of three sub tools: (1) a database to archive information about incidents and thereby monitor reliability, (2) an internal survey to monitor motivation and (3) an assessment to monitor experiential knowledge. Due to practical considerations behaviour should not be monitored. This decision does not have far reaching consequences. Behaviour is monitored indirectly given that is succeeds two monitored variables (motivation and knowledge) and is prior to another variable (reliability). The first sub tool facilitates systematic storing of data about incidents. This data could be used to present employees with the (financial) impact of single incidents and consequently enhance employee's judgement as to what behaviour is appropriate. Additionally, the first sub tool can determine the reliability level of the organization and provide insights in incidents that threaten Oxilion. The second and third sub tool facilitate a half-yearly evaluation of employee's motivations and a half-yearly assessment of experiential knowledge respectively. These tools can by used to decide whether initiatives for improvement should be deployed and, if so, on what aspects these initiatives should focus.

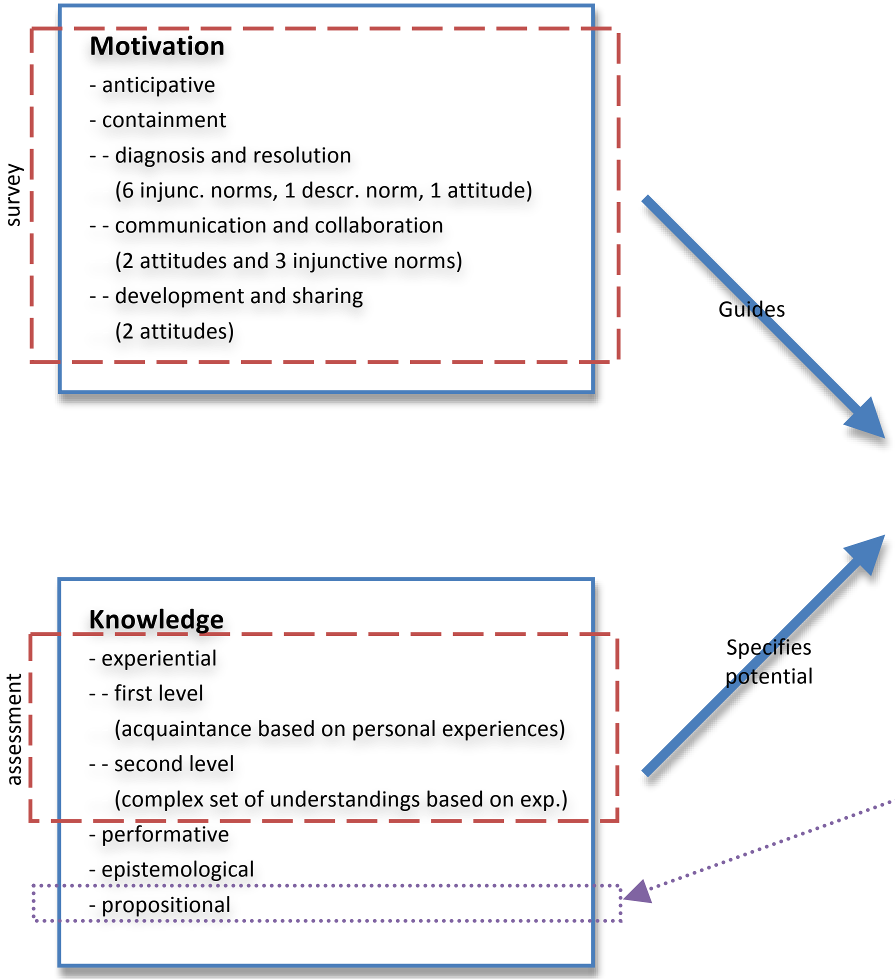
The monitoring tool cannot only be used to monitor reliability, motivation and knowledge, it could also be used as a learning tool that in turn may lead to an improvement of reliability. As a result, the third research questions is:

> *RQ 3*: How can information acquired by the monitoring tool be used to learn and consequently improve reliability?

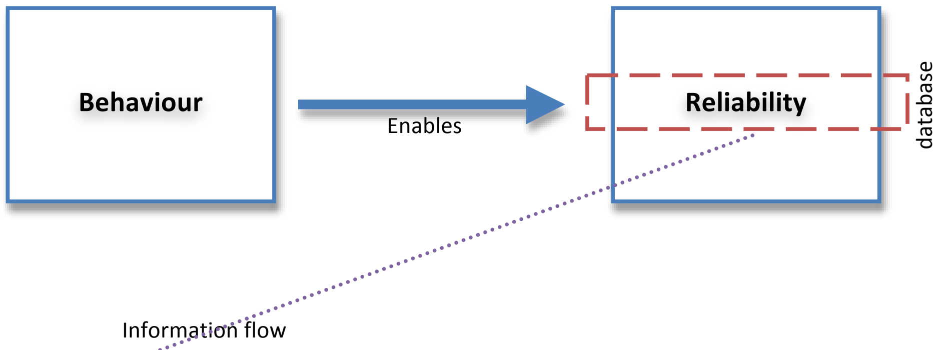
This study focused on the learning potential of the incident database. The database's capacity to systematically record all kinds of information serves two functions: (1) aiding in more effective error-correction (single-loop learning) and (2) facilitating the development of new strategies to manage incidents (double-loop learning). The first function, error-correction, is based on the notion that the incident database could be a valuable source of resolution strategies for reoccurring incidents. As a starting point, one must assume that the first time an incident occurs, its resolution strategy is added to the database. Subsequently, employees that come across the same incident can easily select the resolution strategy from the database and implement the solution. Hence, the database can aid more effective error-correction given that employees don't have to, so to say 'reinvent the wheel', but can simply select and implement a working resolution strategy. However, most incidents employees faced were never encountered before. A strategy to manage these incidents would therefore not be available. Employees would thus need to innovate and develop new strategies. This can be aided by the second function of the database. By combining stored strategies and developing these into a new strategy employees are able handle novel incidents. The more employees pass trough double-loops, the more strategies are stored in the database. Hence, the more the company learns, the more incidents it is able to cover. If aggregated, the information stored in the database might lead to new insights and discussions about the current way of learning. The organization might discover that the current learning style does not fit the learning needs of its rapid changing environment and consequently engages in deutero learning (learning to learn).

Figure 15 on the next page illustrates the research model including (a simplification of) the study's conclusions.

Figure 15: research model including (a simplification of) the study's conclusions


survey
Motivation
- anticipative
- containment
- - diagnosis and resolution
(6 injunc. norms, 1 descr. norm, 1 attitude)
- - communication and collaboration
(2 attitudes and 3 injunctive norms)
- - development and sharing
(2 attitudes)
Guides
assessment
Knowledge
- experiential
- - first level
(acquaintance based on personal experiences)
- - second level
(complex set of understandings based on exp.)
- performative
- epistemological
- propositional
Specifies
potential

↙**Description**: The squires with the solid lines represent the model as described in the theoretical framework. The aspects that constitute appropriate motivation and knowledge are described in depth. A single – denotes a main category, while a double - denotes a sub category of either motivation or knowledge. The squires with the dotted lines illustrate the monitoring tools. An additional dotted arrow is depicted to signal that the monitoring tool of reliability provides real time information and thereby constitutes to the development of propositional knowledge. Note however, that the other tools provide periodic information. For the sake of simplicity this is not depicted.



6.2 LIMITATIONS

At this point, one should make some critical remarks and identify the limitations of this study. The main limitation is its limited scope. Only one organization was studied. This decreases the ability to generalize the findings of this study to other hosting providers or high reliability organizations in general. However, given the study's explorative nature, focussing on one organization was a logical choice. This enabled the researcher to view real-life operations in an organization at close quarters, get insights about its details and develop a nuanced theory. This theory would be difficult to produce and explain if he had insufficient understanding about the organization's context, its operations and interactions between organizational entities.

The second limitation of this study was the complexity and novelty of its context. The context of this study, meaning the company's branch, was not (yet) described by other studies. Although this resulted in a unique contribution to science, resulted it also in an inability to position the branch and the company within existing models developed by past literature. Generally accepted models to describe IT-infrastructure were often not applicable and all-purpose models were too general to explain the challenges and relationships in the branch. The inability to position the branch and the unit of analysis within existing models frustrates a comparison with branches and organizations described in past literature.

The narrow focus on anticipative motivations posed another limitation. In comparison to containment motivations, anticipative motivations were relatively little analysed. The main research method of this study (the research diary method) focussed on genuine incidents that had threatened reliability. This implies that the data gathered with this method did not include any anticipative motivations since anticipative motivations are aimed at spotting potential flaws before they have occurred. In other words: the gathered data with the diaries did only include containment motivations. However, anticipative motivations were assessed with the survey (although less in-depth and less specific).

A fourth limitation of this study is the method used to analyse employee's behaviour. Behaviour was analysed by coding the actions as described in employees' dories. The disadvantage of this method is that only described behaviour was analysed. Actions that were perceived as trivial by employees might not have been entered in the diary and were consequently not taken into account during the analysis. Better methods (e.g. observing employee's behaviour or interviewing employees) would have met with all kind of practical objections due to the volume of incidents (e.g. time-constraints, limited research resources and excessive investment of employee's time).

6.3 CONTRIBUTIONS TO PRACTICE AND THEORY

Despite its limitations, this study contributed to practice and theory. The practical contributions consist mainly of advice for Oxilion and designed tools that aid the organization in monitoring and learning. The first contributed to practice entailed mapping motivations needed to guide appropriate behaviour and knowledge needed in order to show appropriate behaviour. These insights could be used as input for Oxilion's human resource management. Based on this information the organization can deploy initiatives to enforce appropriate motivations and develop appropriate knowledge. Additionally, the study contributed to practice by providing a tool to monitor and learn from reliability. The designed sub tools can monitor changes in motivations, knowledge and reliability. This information can be used to decide whether initiatives for improvement should be deployed and, if so, on what aspects these initiatives should focus. Additionally, the study explained how Oxilion could learn from monitoring reliability. By storing information about incidents and reusing this information for managing reoccurring and novel incidents the company can contain the effects of incidents faster and better, thereby improving reliability. This is a valuable contribution given that Oxilion's customers acknowledge reliability to be the most important aspects of hosting. The fact that the organization has decided to implement the tool signals its significance. Lastly, the study contributed to practice by creating awareness about the potential impact of incidents (especially financial impact) and the overall reliability level of Oxilion. These insights made employees more aware of the importance of managing incidents appropriately.

This study contributed to theory by exploring novel issues in a branch that received limited attention from the research field, and by exploring high reliability issues in a SME. Previous studies conducted in the research field of high reliable organizations focussed on large organizations (probably because high reliably SMEs were nonexistent). This study proposed that the growing dependence of society on the internet gave breed to a new group of high reliability organizations that are relatively small. By focussing on one of these organizations this study contributed to filling a gap in existing literature. Additionally, this study contributed to theory by relating reliability directly to behaviour, motivation and knowledge. These concepts were never incorporated into one model, although previous studies have addressed the relationships separately. However, by developing one theoretical model and supporting this by genuine practical examples, the study provided a unique contribution to literature. Lastly, this study contributed to theory by focussing on a branch that was, until now, relatively underexposed by literature. The contribution entailed the development of a new model to describe the common product offering of hosting providers and a new model to describe the relationships between companies that constitute the hosting branch.

6.4 SUGGESTIONS FOR FUTURE RESEARCH

The insights provided by this study might raise new questions and this study might therefore lead to new research. This study puts forward a couple of suggestions of future research.

This study analysed data from only one hosting provider. Naturally, this calls for a study encompassing data from multiple providers that examines whether the developed theory can be generalized to other hosting providers. If the theory can indeed be generalized to other providers, it can be used as a 'guide' that illustrates how a provider should organize and manage their company in order to achieve high reliability. Given that reliability is the most important performance indicator for a provider, this 'guide' would be a valuable contribution to practice.

Since all hosting providers face (to some degree) the same challenges as discussed in this study, the developed theory might be generalized to other hosting providers. Hence, similar configurations of motivations and knowledge may be found in other hosting providers, and the interrelations between the variables may be the same as described in this study. However, there is possibly a significant difference in how motivation and knowledge are managed in a small hosting provider (SMEs) compared to how these variables are managed in a large hosting provider. The study demonstrated that Oxilion's management stimulated appropriate motivation by setting an example, working together with employees and meeting with all employees on a regular basis (page 40). Appropriate motivations were thus mainly stimulated informally. This mode of stimulating motivations might not work in a large hosting provider. Due to the organization's size, its management might be unable to communicate appropriate motivations effectively. This implies that large providers would need other 'mechanisms' to stimulate appropriate motivations. Appropriate motivations might need to be stimulated formally (e.g. written rules) or by rewarding employees (e.g. issuing bonuses or choosing an employee of the month).

Additionally, large providers might need to manage knowledge differently than small providers. The study demonstrated that Oxilion's employees knew from personal experiences (acquaintances) that a specific colleague could help them. In other words, employees were able to locate knowledge because they had an (intangible) overview of all knowledge residing in the organization. It is likely that employees of large providers do not have this overview since it would be unlikely that they are acquainted with all colleagues. This implies that employees might be unable to locate essential knowledge. Therefore, the provider might be required to map all knowledge, label it (e.g. novice, expert or guru in technology X) and create 'yellow pages' that employees can use to get in contact with the right colleague.

Furthermore, a study conducted in multiple hosting providers could contribute to the development of an industry-wide standard. Based on the reliability level of multiple hosting providers one might be able to establish a standard reliability level. With this standard one would be able to compare the performance of providers. Hosting providers could use this level to determine how they stack up against their competitors. Additionally, if made public, consumers and businesses could use the standard to compare providers and consequently make a more balanced decision when they are looking for a suitable provider ('do I chose the expensive but reliable provider or do I chose the cheap but less reliable provider?'). Hence, a standard reliability level would contribute to a more transparent hosting branch.

Additionally, a study or series of studies should be conducted to test whether the developed theory could be generalized to other high reliability organizations that do not operate in the hosting branch. Previous studies demonstrated that high reliability organizations are generally large private businesses or large (semi) governmental organisations. These organizations might face totally different business challenges than hosting providers. Due to the difference in size and business challenges, these organizations require probably different configurations of behaviour, motivations and knowledge. The knowledge configuration of a large organization, for example, might differ substantially compared to the knowledge configuration of a small organization. Large organizations described in previous literature included: aviation services (e.g. Burke, Wilson, & Salas, 2005), space aviation agencies (e.g. Starbuck & Farjoun, 2005), health care clinics (e.g. Xiao, Plasters, Seagull, & Moss, 2002) and nuclear power plants (e.g. Svenson, Salo, Oedewald, Reiman, & Skerve, 2006). The employees of these organizations are probably all trained in an educational programme especially tailored to the knowledge needed in these organizations. As a consequence, one would thus expect that employees who work in these organization use knowledge learned during formal education more often. In other words: whereas employees in a hosting provider might rely almost solemnly on their experience, employees in these organizations might rely on epistemological knowledge in addition to experiential knowledge.

The text above described that employees in a hosting provider might rely almost solemnly on their experience. The study demonstrated that at Oxilion this is indeed true. The technology used by Oxilion is either too specific or too much the subject of change to be learned in nearly all types of formal education. Given that, in general, other providers work with similar technology as Oxilion, this finding might be generalized to other hosting providers. This would imply that no formal educational programme is suited to train (future) employees of a hosting provider. Therefore, this study proposes a study that explores how formal education can be better suited to match the knowledge needed by a hosting provider. This study could reduce the need to train (starting) employees on the job given that they already have acquired (some) knowledge during their formal educational programme.

Additionally, this study proposes that the perceptual impact of incidents is explored more intensively. The study demonstrated that incidents could influence public perception about a provider. However, this dimension of impact was only motioned briefly (given that is difficult to determine its impact accurately). This study proposes that the impact of incidents on public perception about a provider (a provider's reputation) should be studied more in depth. In a branch where reliability is key, an unreliable reputation might have a devastating effect. Large incidents might lead to bad press, which in turn might lead to a damaged reputation. Depending on the size of the incidents, the reputational damage done might be so great that the provider is unable to acquire new customers. The perceptual impact of small incidents might be minor. However, as the number of customers involved in an incident increases and the intensity of the technical impact of the incidents growths, the perceptual impact of the incidents might grow exponentially. With very large incidents a provider's reputation might be so damaged that has difficulty overcoming its unreliable reputation.

REFERENCES

Ajzen, I. (1991). The theory of planned behaviour. *Organizational behavior and human decision processes , 50*, 179 - 211.

Ajzen, I., & Fishbein, M. (2005). The influence of attitudes on behavior. In D. Albarracin, B. Johnson, & M. Zanna, *The handbook of attitudes* (pp. 173 - 222). Mahwah: Lawrence Erlbaum Associates Inc. Publishers.

Alavi, M., & Leidner, D. (2001). Knowledge management and knowledge systems: conceptual foundations and research issues. *MIS Quarterly , 25* (1), 107 - 136.

Barua, A., Pinnell, J., Shutter, J., & Whinston, A. (1999). *Measuring the internet economy: an exploratory study.* Austin: University of Texas.

Beeby, M., & Booth, C. (2000). Networks and inter-organizational learning: a critical review. *The learning organization , 7* (2), 75 - 88.

Blatt, R., Christianson, M., Sutcliffe, K., & Rosenthal, M. (2006). A sensemaking lens on reliability. *Journal of organizational behaviour , 27* (7), 897 - 917.

Burke, C., Wilson, K., & Salas, E. (2005). The use of a team-based stratgey for organizational transformation: guidance for moving toward a high reliablity organization. *Theoretical issues in ergonomics science , 6* (6), 509 - 530.

Chakrabarti, A., & Manimaran, G. (2002). Internet infrastructure security: a taxonomy. *IEEE network , 16* (6), 13 -21.

Cialdini, R. (2003). Crafting normative messages to protect the environment. *Current directions in psychological science , 12* (4), 105 - 109.

Creswell, J. (2007). Editorial: mapping the field of mixed method research. *Journal of mixed method research. , 3* (2), 95 -108.

Creswell, J. (2009). *Research design: qualitative, quantitative and mixed methods approaches.* Los Angeles: Sage Publications.

Eurostat. (2009). *European business - facts and figures.* Luxembourg: Office for official publications of the european communities.

Freeman, R. (2007). Epistemological bricolage how practitioners make sense of learning. *Administration & Society , 39* (4), 476 - 496.

Hopkins, A. (2007). The problem of defining high reliablity organisations. *Working paper 51* , 1 - 14.

Huttner, S. (2007). The internet economy: Towards a better future. *OECD Observer , 263*, 1 - ?

ISPam. (2009 26-August). *De huidige stand van zaken op de Nederlandse hostingmarkt*. Retrieved 2010 5-July from ISPam.nl: http://www.ispam.nl/archives/12302/de-huidige-stand-van-zaken-op-de-nederlandse-hostingmarkt/

Jaccard, J., & Blanton, H. (2005). The origens and structure of behavior: conceptualizing behaviors in attitude research. In D. Albarracin, B. Johnson, & M. Zanna, *The handbook of attitudes* (pp. 125 - 172). Mahwah: Lawrence Erlbaum Associates Inc. Publishers.

Johnson, R., & Onwuegbuzie, A. (2004). Mixed methods research: a research paradigm whose time has come. *Educational researcher , 33* (7), 14 - 26.

Johnson, R., Onwuegbuzie, A., & Turner, L. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research , 1* (2), 112 - 133.

Kim, M., & Hunter, J. (1993). Attitude-behavior relations: a meta-analysis of attitudinal relvance and topic. *Journal of communication , 43* (1), 101 - 142.

Kruglanski, A., & Stroebe, W. (2005). The influence of beliefs and goals on attitudes: issues of structure, function and dynamics. In D. Albarracín, B. Johnson, & M. Zanna, *The handbook of attitudes.* (pp. 323 - 368). Mahwah: Lawrence Erlbaum Associates Inc. Publishers.

LaPorte, T. (1996). High reliability organizations: unlikely, demanding and at risk. *Journal of contingencies and crisis management , 4* (2), 60 - 71.

LaPorte, T., & Consolini, P. (1991). Working in practice but not in theory: theoretical challenges of high-reliability organizations. *Journal of public administration research and theory , 1* (1), 19 - 48.

Leveson, N., Dulac, N., Marais, K., & Carroll, J. (2009). Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems. *Organizations studies , 30* (2/3), 227 - 249.

Lucas, H., & Sylla, R. (2003). The global impact of the internet: widening the economic gap between wealthy and poor nations? . *Prometheus , 21* (1), 1 -22.

Meyer, B., & Sugiyama, K. (2006). The concept of knowledge in KM: a dimensional model. *Journal of knowledge management , 10* (6), 1 - 22.

Mingers, J. (2008). Management knowledge and knowledge management: realism and forms of truth. *Knowledge management research & practice , 6*, 62 - 76.

OECD. (2009). *Information technology outlook 2008.* Paris: OECD Publishing.

OECD. (2008). The Future of the Internet Economy. *OECD Ministerial meeting. 268*, pp. 1 - 8. Seoul: OECD Observer.

Rivis, A., & Sheeran, P. (2003). Descriptive norms as an additional predictor in the theory of planned behaviour: a meta-analysis. *Current Psychology , 22* (3), 218 - 233.

Roberts, K. (1990). Managing high reliability organizations. *California management review , 32* (4), 101 - 113.

Roberts, K., & Rousseau, D. (1989). Research in nearly failure-free, high-reliability organizations: having the bubble. *IEEE transactions of engineering management , 36* (2), 132 - 139.

Rochlin, G. (1993). Defining high reliability organizations in practice: a taxonomic prologue. In K. Roberts, *New Challenges to Understanding Organizations* (pp. 11 - 32). New York: Macmillan CTD.

SIDN. (2010). *Jaarverlslagen.* Arnhem: SIDN.

SIDN. (2010 26-Februari). *Registrars Alfabetisch*. Retrieved 2010 26-Februari from SIDN: https://www.sidn.nl/over-nl/registrar-zoeken/registrars-alfabetisch/

SIDN. (2010 25-May). *Statistieken*. Retrieved 2010 5-Juli from SIDN.nl: https://www.sidn.nl/kennisbank/statistieken/

Starbuck, W., & Farjoun, M. (2005). *Organization at the limit: lessons from the coumbia disaster.* Malden, USA: Blackwell.

Sullivan, J., & Beach, R. (2009). Improving project outcomes trough operational reliability: a conceptual model. *International journal of project management , 27* (8), 765 -775.

Svenson, O., Salo, I., Oedewald, P., Reiman, T., & Skerve, A. (2006). *Nordic perspective on safety management in high reliability organizations.* Roshilde: NKS Secretariat.

Symon, G. (2004). Qualitative research diaries. In C. Cassell, & G. Symon, *Essential guide to qualitative methods in organizational research* (pp. 98 - 113). London: SAGE Publications Ltd.

Synovate. (2009). *Vijftien jaar internet. Wat heeft het voor ons betekend?* Amsterdam: Synovate BV.

Van Bon, J. (2008). *IT service management based on ITIL® V3: een pocketguide.* Zaltbommel: Van Haren Publishing.

Visser, M. (2007). Deutero-learning in organizations: a review and reformulation. *Academy of management review , 32* (2), 659 - 667.

Weick, K., & Sutcliffe, K. (2007). *Managing the unexpected: resilient performance in an age of uncertainty.* San Fransisco: Jossey-Bass.

Weick, K., Sutcliffe, K., & Obstfeld, D. (1999). Organizing for high reliability: processes of collective mindfulness. In A. Boin, *Crises management* (pp. 31 - 66). London: Sage Publications Ltd.

Wijnhoven, F. (2001). Acuiring organizational learning norms: a contingency approach for understanding deutero learning. *Management Learning , 32* (2), 181 - 200.

Wijnhoven, F., Schuur, P., & Timmer, J. (2010). The inventor game: game-theoretical analysis of knowledge-sharing between inventors and employers. *Knowledge management research & practice. , 8* (1), 61 -75.

Xiao, Y., Plasters, C., Seagull, F., & Moss, J. (2002). Cultural and institutional conditions for high reliablity teams. *IEEE international conference on systems, management and cybernetics*, (pp. 2580 - 2585). Delft.

Yan, G., Eidenbenz, S., Thulasidasana, S., Datta, P., & Ramaswamy, V. (2009). Criticality analysis of internet infrastructure. *Computer networks , 54* (7), 1169 - 1182.

APPENDICES

APPENDIX A: RESULTS OF THE DIARY RESEARCH METHOD

Incident Reg.				Incident Information														
				Description	Reliability						Behaviour				Motivation		Knowlegde	
Week	Number	Sort			Tech. per imp. (cat)	Tech. per. imp. (desc.)	Fin. impact (cat)	Root cause	Software = people failure	Fin. impact (nominal)	Action	Object/enitity	Aimed at	ITIL	Description	Norm	Form of knowledge	Exper Level 1 or 2
18	1	network		dos-attack	3	reduced performance	D	E		€75,100	asking	colleague	P	C	learn from incident	AT	propositional	
											configuring	server	H	D	share knowledge	AT	experiential	1,2
											rebooting	server	H	D	react quickly	IN		
											modifying	network	H	D				
	2	san		freeze san management	4	limited admin control	E	S	PE	€11,000	searching	logs	A	C	double-check	IN	experiential	1,2
											calling	helpdesk	P	C	react quickly	IN	propositional	
											clearing	server	H	D			epistemological	
	3	e-mail		spam run	3	reduced performance	D	S	PC	€97,000	suspending	user account	A	C	react quickly	IN	experiential	1,2
											consulting	colleague	P	C	double-check	IN	propositional	
											deleting	user account	A	D				
	4	server		limited employees av.	5	risk	E	O		€10,000	prioritizing	tasks	A	B			experiential	1
											consulting	colleague	P	C			propositional	
	5	e-mail		adressbook unavailable	3	reduced performance	C	S	PM	€100,000	searching	solution	S	C	help others	IN	propositional	
											restoring	software	S	D			experiential	2
	6	control p.		upgrade plesk	5	risk	E	S	PE	€600	upgrading	software	S	D	double-check	IN	experiential	2
	7	nr																
19	8	mon. tool		reinstall monitoring tool tool	4	limited admin control	D	S	PE	€96,000	turning off	service monitoring tool	S	C	learn from incident	AT	experiential	2
											turning off		S	C				
	9	acess list		old IP's on access list	5	risk	A	A		€200,000	deleting	IP's	A	D			experiential	2
	10	nr																
	11	nr																
20	12	control p.		webinterface plesk broken	2	loss of functionality	C	S	PM	€100,400	upgrading	software	S	D	upgrade when enc. failures	DN	experiential	2

	13	server	server down	1	downtime	C	H		€111,360	rebooting	server	H	D			experiential	2
	14	server	virt server froze	1	downtime	E	S	PE	€420	rebooting	virt. server	S	D	learn from incident	AT	experiential	2
	15	server cl.	management server down	2	loss of functionality	A	H		€200,000	replugging	server	H	D	be carefull	IN	performative	
21	16	server cl.	host VDS on VDC	5	risk	A	S	PE	€200,000	informing	colleague	P	B	questioning	AT	experiential	1
	17	nr															
22	18	server	control panel down	2	loss of functionality	E	S	PM	€3,000	upgrading	software	S	D	upgrade when enc. failures	DN	experiential	2
	19	nr															
	20	e-mail	spam run	3	reduced performance	C	S	PC	€110,400	checking	monitoring tool	S	C	react quickly	IN	experiential	2
										searching	script	S	C	limit futher damage	IN		
										removing	script	S	D	double-check	IN		
										restoring	files	S	D				
	21	server cl.	overload of virt. Node	3	reduced performance	E	S	PE	€40,800	migrating	virt. Server	S	D	find permanent solution	IN	experiential	2
										checking	load	S	D	limit futher damage	IN		
	22	server	migration of virt. Server	1	downtime	E	S	PE	€5,400	removing	files	S	D	learn form incident	AT	experiential	2
	23	nr															
23	24	nr															
	25	e-mail	spam run	3	reduced performance	C	S	PC	€115,200	checking	monitoring tool	S	C	react quickly	IN	experiential	2
										restoring	files	S	D				
										clearing	mail queue	A	D				
	26	control p.	upgrade control panel	1	downtime	E	S	PE	€6,000	upgrading	software	S	D	find permanent solution	IN	experiential	2
										restarting	service	S	D	inform customers timely	IN		
24	27	e-mail	filiter is too strict	3	reduced performance	E	S	PE	€15,000	informing	colleague	P	B	questioning	AT	experiential	1,2
										consulting	colleague	P	C	share knowledge	AT		
										deleting	IP's	A	D				
	28	san	hard disk failure	5	risk	E	H		€10,000	calling	helpdesk	P	D			propositional	
										installing	hard disk	H	D			performative	
	29	server cl.	upgrade virt. Server	5	risk	B	S	PM	€163,200	isolating	server	H	D	inform customers timely	IN	experiential	2
										upgrading	software	S	D			epistemological	
	30	control p.	upgrade control panel	1	downtime	C	S	PM	€120,000	upgrading	software	S	D	limit futher damage	IN	experiential	2
25	31	network	ddos-attack	3	reduced performance	D	E		€74,100	modifying	network	H	D			experiential	2
	32	operating s.	instability RHEV	1	downtime	E	S	PM	€1,260	configuring	server	H	D	learn from incdient	AT	experiential	2
										upgrading	software	S	D	inquire issues	IN		
	33	e-mail	spam run	3	reduced performance	C	S	PC	€120,000	checking	monitoring tool	S	C			experiential	2

										restoring	files	S	D				
										removing	script	S	D				
	34	datacenter	datacenter Enschede down	1	downtime	A	H		€200,000	prioritizing	tasks	A	B	inform customers timely	IN	propositional	
										coordinating	tasks	A	B	questioning	AT	experiential	1
										rebooting	server	H	D	learn from incident	AT	performative	
										checking	server	H	D	help others	IN		
	35	nr															
26	36	e-mail	spam run	3	reduced performance	C	S	PC	€132,000	checking	monitoring tool	S	C	limit futher damage	IN	experiential	2
										restoring	files	S	D	react quickly	IN		
										clearing	mail queue	A	D				
	37	server	snapshot active/red. Perfor	3	reduced performance	E	S	PC	€4,800	removing	files	S	D			epistemological	
27	38	san	power supply failure	5	risk	A	H		€200,000	checking	power supply	H	C			performative	
										taking out	power supply	H	D				
										installing	power supply	H	D				
	39	e-mail	spam-run	3	reduced performance	D	S	PC	€97,000	disabling	user account	A	D			experiential	2
	40	operating s.	bug in OS	3	reduced performance	E	S	PM	€6,200	informing	colleague	P	B	questioning	AT	experiential	1,2
										calling	helpdesk	P	C	inquire issues	IN		
										configuring	san	H	D	find permanent solution	IN		
	41	operating s.	bug in OS	2	loss of functionality	E	S	PE	€6,400	informing	colleague	P	B	questioning	AT	propositional	
										calling	helpdesk	P	C	discussion	AT	experiential	1,2
										configuring	software	S	D				
	42	san	limited recources	2	loss of functionality	E	O		€9,600	informing	colleague	P	B	questioning	AT	propositional	
										ordering	server	H	D			experiential	1
	43	san	new manufacture	5	risk	E	H		€11,000	informing	colleague	P	B	questioning	AT	propositional	
										warning	colleague	P	B	discussion	AT	experiential	1
28	44	e-mail	spam run	3	reduced performance	C	S	PC	€132,000	checking	monitoring tool	S	C			experiential	2
										searching	script	S	C				
										removing	script	S	D				
										restoring	files	S	D				
										clearing	mail queue	A	D				
	45	server cl.	reduced redundancy	3	reduced performance	E	O		€7,560	migrating	virt. Server	S	D	find permanent solution	IN	experiential	2
	46	operational	limited personnel support	5	risk	E	O		€8,000	coordinating	tasks	A	B	help others	IN	propositional	
																experiential	1

	47	operational		limited personnel technique	5	risk	E	O		€11,000	prioritizing	tasks	A	B	limit futher damage	IN	experiential	1
29	48	server cl.		vdc cluster ofline	1	downtime	E	S	PM	€42,000	configuring	software	S	D	inquire issues	IN	experiential	1,2
											calling	helpdesk	P	D			propositional	
	49	san		san full	3	reduced performance	D	O		€63,000	migrating	virt. Server	S	D	find permanent solution	IN	experiential	2

APPENDIX B: RESULTS OF THE INTERNAL SURVEY

Preoccupation with failure 'paying attention to weak signals'	1	We zijn constant alert op potentiële fouten binnen onze organisatie en proberen ze te begrijpen.	5	4	3	4	4	4	4	4	4	5	4	4	4,1
	2	Als er iets onverwachts gebeurt proberen we altijd uit te zoeken waarom het anders liep dan verwacht.	5	5	4	3	5	5	5	5	5	4	5	4	4,6
	3	We beschouwen kleine gebreken als een indicatie voor potentiële grote fouten in plaats van het bewijs dat we erg goed zijn in het ontdekken van kleine gebreken.	5	2	3	3	3	5	4	3	4	1	3	3	3,3
	4	We updaten vaak onze werkwijzen naar aanleiding van een fout.	4	4	2	4	4	5	5	4	4	3	4	4	3,9
	5	Als je een fout maakt wordt je daar niet op afgerekend.	4	4	3	3	3	4	3	1	3	4	4	3	3,3
	6	Mensen rapporteren grote fouten, ook als de fout nog niet door anderen is ontdekt.	5	4	3	4	4	4	5	3	2	4	5	5	4,0
	7	Managers zijn actief op zoek naar zaken die mogelijk tot probleem kunnen leiden	5	4	2	3	5	4	4	2	4	2	4	3	3,5
	8	Mensen voelen zich vrij om met hun manager te praten over problemen	5	5	4	4	5	5	5	4	4	5	5	5	4,7
	9	Mensen worden beloond als ze potentiële problemen ontdekken	4	3	4	3	2	5	4	2	3	2	2	4	3,2
			4,7	3,9	3,1	3,4	3,9	4,6	4,3	3,1	3,7	3,3	4,0	3,9	3,8

Reluctance to simplify 'differentiation in views and mindsets'	1	Mensen beschouwen hier niets als vanzelfsprekend	4	2	3	3	2	2	5	3	4	4	5	4	3,4
	2	Het ter discussie stellen van bepaalde zaken wordt aangemoedigd.	5	4	4	3	3	4	5	4	5	5	5	4	4,3
	3	We streven er naar om de status-quo te doorbreken.	4	4	4	4	4	4	5	2	5	3	4	5	4,0
	4	Mensen voelen zich vrij om problemen of lastige zaken ter sprake te brengen.	5	5	4	4	4	5	4	4	5	5	4	4	4,4
	5	Mensen verdiepen zich altijd meer in een probleem dan strikt noodzakelijk om de aard van problemen beter te begrijpen.	4	2	2	2	4	4	4	5	4	3	4	4	3,5
	6	Mensen worden aangemoedigd om verschillende standpunten ter sprake te brengen	4	4	4	3	3	4	5	2	4	4	5	4	3,8
	7	Mensen luisteren aandachtig, het komt zelden voor dat iemands visie wordt genegeerd.	5	2	3	4	2	3	4	4	4	3	5	3	3,5
	8	Mensen worden niet 'aangevallen' als ze iets rapporteren dat kan leiden tot een onderbreking van normale bedrijfsprocessen.	4	4	4	4	4	4	4	4	2	2	4	4	3,7
	9	Als er iets onverwachts gebeurt richten mensen zich op de analyse van het probleem in plaats van het promoten van hun standpunt.	4	2	2	3	3	4	5	2	5	3	5	5	3,6
	10	Sceptici worden zeer gewaardeerd.	4	4	3	1	3	4	4	2	4	4	4	4	3,4
	11	Mensen vertrouwen elkaar.	4	4	4	3	5	5	5	2	4	4	5	4	4,1
	12	Mensen hebben respect voor elkaar.	5	4	3	4	4	5	5	3	4	4	5	4	4,2
			4,3	3,4	3,3	3,2	3,4	4,0	4,6	3,1	4,2	3,7	4,6	4,1	3,8

Sensitivity to operations 'having a cognitive map of the current situations and implications for the future'	1	Er is altijd wel iemand die weet hoe de organisatie er voor staat.	5	4	4	4	5	5	5	4	5	5	5	5	4,7
	2	Als er problemen ontstaan is er altijd wel een manager beschikbaar voor vragen.	5	5	4	4	2	5	5	3	5	5	5	4	4,3
	3	Managers staan klaar om te helpen mocht dit nodig zijn.	5	4	4	5	4	5	5	5	5	4	5	4	4,6
	4	Mensen zijn vrij om naar eigen inzicht onverwachte problemen op te lossen.	5	3	4	4	5	5	5	4	4	4	3	5	4,3
	5	Doorgaans werken mensen voldoende met elkaar om een goed beeld te krijgen van de huidige stand van zaken binnen de organisatie.	4	4	3	4	3	4	4	3	5	4	4	4	3,8
	6	Mensen vragen altijd om feedback over zaken die niet goed gaan.	4	2	4	4	4	4	4	2	4	4	4	4	3,7
	7	Mensen zijn bekend met andermans taken.	5	2	2	5	4	4	4	2	4	4	5	3	3,7
	8	We hebben de beschikking over allerlei middelen als er iets onverwachts gebeurt.	4	3	3	3	5	4	4	4	4	3	4	4	3,8
	9	Managers houden constant de werklast in de gaten en verlagen de werklast als die te hoog wordt.	4	4	4	4	1	4	4	2	4	3	3	3	3,3
			4,6	3,4	3,6	4,1	3,7	4,4	4,4	3,2	4,4	4,0	4,2	4,0	4,0

Commitment to resilience 'preserve functioning, recover and learn form previous'	1	Er zijn constant middelen beschikbaar voor het trainen van technische werknemers.	4	5	4	4	3	4	4	3	4	4	5	4	4,0
	2	Mensen beschikken over voldoende kennis en kunde voor het werk wat ze doen.	5	4	5	4	5	4	4	5	4	4	4	5	4,4
	3	De organisatie is actief betrokken bij het ontwikkelen van de vaardigheden en kennis van haar werknemers.	5	4	3	5	4	4	5	3	5	5	5	5	4,4
	4	Deze organisatie moedigt het oppakken van uitdagende langlopende projecten aan.	4	4	4	4	4	4	5	4	5	5	5	4	4,3
	5	Mensen in deze organisatie staan bekend om hun innovativiteit.	3	4	4	5	5	5	5	5	4	3	4	5	4,3
	6	Deze organisatie draagt zorg voor het ontwikkelen van de expertise van haar werknemers.	5	4	4	4	3	4	5	4	5	4	4	5	4,3
	7	We beschikken over een aantal informele contacten die we soms inzetten om problemen op te lossen.	5	2	3	5	4	4	5	4	4	3	3	5	3,9
	8	Mensen in deze organisatie leren van hun fouten.	5	3	3	4	4	5	4	4	5	4	5	4	4,2
	9	We zijn afhankelijk van elkaar.	5	4	4	4	5	4	4	3	4	4	5	4	4,2
	10	De meeste werknemers beschikken over voldoende vaardigheden om op onverwachte problemen in te spelen.	5	4	5	4	4	5	5	4	4	5	4	4	4,4
			4,6	3,8	3,9	4,3	4,1	4,3	4,6	3,9	4,4	4,1	4,4	4,5	4,2

Comment: this study focused on containment motivations (represented by the items in the tables 'Commitment to resilience' and 'Deference to expertise' on the next page). The items that scored (on average) higher than a four (coloured cells) were used as input for the classification of motivations needed to guide appropriate behaviour (Appendix F)

Deference to expertise 'assigning problems to employees/ units with the most expertise'	1	Mensen zijn toegewijd aan hun werk.	5	4	4	4	5	4	4	4	5	5	5	5	4,5
	2	Mensen respecteren andermans werk.	5	2	4	5	4	4	5	2	4	5	5	4	4,1
	3	Als er iets vreemds gebeurd weten werknemers wie ze moeten benaderen om het op te lossen.	5	4	5	5	5	4	5	4	5	5	5	4	4,7
	4	Mensen in deze organisatie hechten meer waarde aan expertise dan van de positie in de organisatie.	5	4	4	5	3	4	4	2	4	4	3	4	3,8
	5	In deze organisatie worden beslissingen gemaakt door de mensen die over de juiste kennis en kunde beschikken.	5	4	4	3	2	4	5	3	5	4	5	4	4,0
	6	Mensen zijn verantwoordelijk voor een probleem tot het probleem is opgelost.	3	4	4	4	3	4	5	5	4	3	5	4	4,0
	7	Het is gemakkelijk om een expert binnen de organisatie te vragen als er zich een probleem voor doet dat we niet kunnen oplossen.	4	4	3	2	5	5	5	5	4	5	5	5	4,3
			4,6	3,7	4,0	4,0	3,9	4,1	4,7	3,6	4,4	4,4	4,7	4,3	4,2

APPENDIX C: CLASSIFICATION OF INCIDENTS BASED ON CAUSE

Cause	Category	Times counted	Percentage
Software	S	26	63%
Hardware	H	6	15%
Administrative	A	1	2%
Operational	O	6	15%
External	E	2	5%
		41	100%

A breakdown of the failures in the software category:

Description	Category	Times counted	Percentage
Failures made by employees	PE	10	38%
Failures made by manufacturers	PM	8	31%
Failures made by customers	PC	8	31%
		26	100%

APPENDIX D: CLASSIFICATION OF BEHAVIOUR BASED ON ITIL

ITIL (and action + entity)		**Category***	**Times counted**	**Percentage**
Incident detection and recording				
-		A	0	0%
Classification and initial support				
prioritizing	tasks			
informing	colleague			
coordinating	tasks			
warning	colleague	B	12	14%
Investigation and diagnosis				
searching	logs			
calling	helpdesk			
suspending	user account			
consulting	colleague			
searching	solution			
turning off	service			
turning off	monitoring tool			
checking	monitoring tool			
searching	script			
checking	power supply	C	20	24%
Resolution and recovery				
configuring	server			
rebooting	server			
modifying	network			
clearing	server			
deleting	user account			
restoring	software			
upgrading	software			
deleting	IP's			
rebooting	virtual server			
replugging	server			
removing	script			
restoring	files			
migrating	virtual server			
checking	load			
removing	files			
clearing	mail queue			
restarting	service			
calling	servicedesk			
installing	hard disk			
isolating	server	D	51	61%
Incident closure				
-		E	0	0%
			83	100%

* Input from ITIL-column in the table of appendix A.

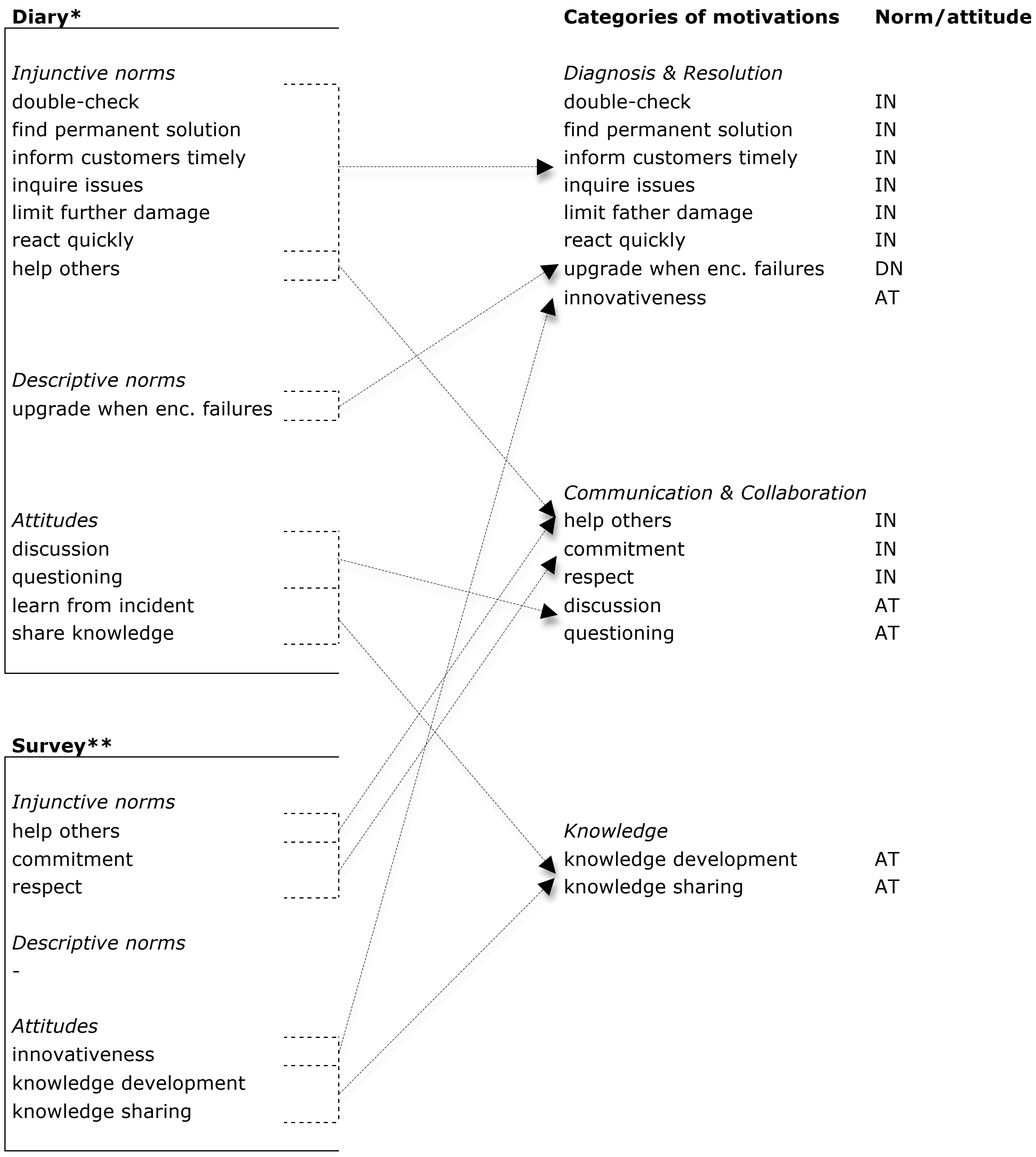
APPENDIX E: CLASSIFICATION OF BEHAVIOUR BASED ON OBJECT AND ENTITY

Description (and action + entity)		**Category***	**Times counted**	**Percentage**
Behaviour directed at software				
checking	monitoring tool			
checking	load			
configuring	software			
migrating	virt. Server			
rebooting	virt. server			
removing	script			
removing	files			
restarting	service			
restoring	software			
restoring	files			
searching	solution			
searching	script			
turning off	service			
turning off	monitoring tool			
upgrading	software	S(oftware)	36	43%
Behaviour directed at hardware				
checking	server			
checking	power supply			
clearing	server			
configuring	server			
configuring	san			
installing	hard disk			
installing	power supply			
isolating	server			
modifying	network			
ordering	server			
rebooting	server			
replugging	server			
taking out	power supply	H(ardware)	17	20%
Behaviour directed at people				
asking	colleague			
calling	helpdesk			
consulting	colleague			
informing	colleague			
warning	colleague	P(eople)	16	19%
Behaviour directed administrative entities				
clearing	mail queue			
coordinating	tasks			
deleting	user account			
deleting	IP's			
disabling	user account			
prioritizing	tasks			
suspending	user account	A(adminst)	14	17%
			83	100%

* Input from column 'aimed at' in the table of appendix A.

APPENDIX F: CODING AND CATEGORIZING OF MOTIVATIONS

This study used the diary collection method and an internal survey to map motivations needed to show appropriate behaviour. The motivations mentioned in employee's diary entries and the motivations assessed with the survey were coded and categorized as following:



Diary*

Injunctive norms
double-check
find permanent solution
inform customers timely
inquire issues
limit further damage
react quickly
help others

Descriptive norms
upgrade when enc. failures

Attitudes
discussion
questioning
learn from incident
share knowledge

Survey**

Injunctive norms
help others
commitment
respect

Descriptive norms
-

Attitudes
innovativeness
knowledge development
knowledge sharing

Categories of motivations	**Norm/attitude**
Diagnosis & Resolution	
double-check	IN
find permanent solution	IN
inform customers timely	IN
inquire issues	IN
limit father damage	IN
react quickly	IN
upgrade when enc. failures	DN
innovativeness	AT
Communication & Collaboration	
help others	IN
commitment	IN
respect	IN
discussion	AT
questioning	AT
Knowledge	
knowledge development	AT
knowledge sharing	AT

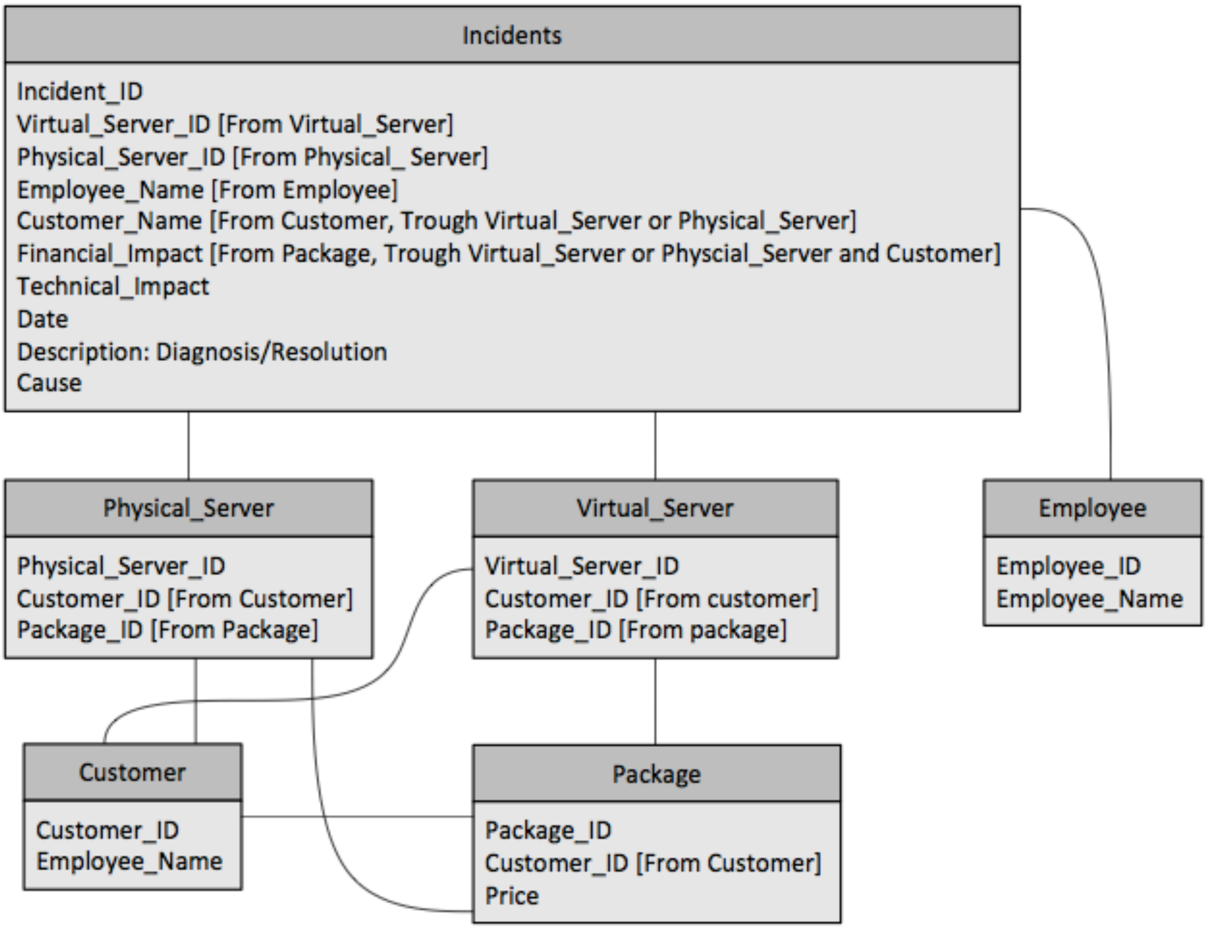
* Only motivations that were mentioned multiple times in the diaries were included.
** Only containment motivations that scored higher than a four were included.

APPENDIX G: INCIDENT DATABASE STRUCTURE

The two figures below depict how data can be entered and stored in the incident database. The upper figure depicts the digital form used to report incidents, whereas the lower figure depicts in which table (in Oxilion's database) the entered data is stored. Employees only need to fill out the items denoted with a *. The other items are filled out automatically.

In order to store the reports a special 'table' (named 'incidents') is created in Oxilion's database. This table contains all the data about reported incidents. However, some data in this table is retrieved from other tables. The name of an employee, for example, is retrieved from the table 'Employees'. Some interrelations are more complex. For example, the name of a customer is retrieved from the table 'Customers' trough either the table 'Virtual_Server' or 'Physical_Server' (depending whether the incident occurred on a virtual or physical server).

Report an incident			
Data:	*Data*	Technical impact*:	*Technical_Impact*
Reported by:	*Employee_Name*	Financial impact:	*Financial_Impact*
System:	*Virutal_Server_ID or Physical_Server_ID*	Customer(s):	*Customer_Name*
Cause*:	*Cuase*		
Diagnosis & Resolution*:	*Description*		


Incidents
Incident_ID
Virtual_Server_ID [From Virtual_Server]
Physical_Server_ID [From Physical_ Server]
Employee_Name [From Employee]
Customer_Name [From Customer, Trough Virtual_Server or Physical_Server]
Financial_Impact [From Package, Trough Virtual_Server or Physcial_Server and Customer]
Technical_Impact
Date
Description: Diagnosis/Resolution
Cause
Physical_Server
Physical_Server_ID
Customer_ID [From Customer]
Package_ID [From Package]
Virtual_Server
Virtual_Server_ID
Customer_ID [From customer]
Package_ID [From package]
Employee
Employee_ID
Employee_Name
Customer
Customer_ID
Employee_Name
Package
Package_ID
Customer_ID [From Customer]
Price

APPENDIX H: MOCK-UP OF AN ANNUAL INCIDENT REPORT

[1] OVERVIEW OF INCIDENTS

Financial Impact

(x € 1000)	Risk	Loss of admin management	Reduced performance	Loss of functionality	Downtime
€ 200				2	
€ 150 - 200					1
€ 100 - 150	2	6			
€ 50 - 100			4		1
€ 0 - 50	5			4	3

Technical Impact

[2] KEY STATISTICS

Total number of incidents: 27
Average: 6,75

Average pot. impact: € 156.000
Median pot. impact: € 42.000

[3] TOP 5 CUSTOMERS INV. IN INCIDENT

#1 - € 245.000 – Name
#2 - € 215.000 – Name
#3 - € 165.000 – Name
#4 - € 123.000 – Name
#5 - € 115.000 – Name

[4] TOP 5 SOURCE OF INCIDENTEN

#1 - SPAM € 430.000
#2 - Plesk interface € 340.000
#3 - VDC Cluster € 230.000
#4 - DOS-Attack € 125.000
#5 - SAN € 75.0000

[5] PREVIOUS MONTHS

```
January              |---------|[####][###########]|-------|

February                       |------|[#########][#####]|-------|

March                                 |------|[####][#####]|----------------|

April                        |-----|[#########][#####]|-------|

May                              |-----------------|[##][#####]|-------|

June                                   |-----------------|[#########][#####]|-------|

                  0 ------------------- 50 ------------------- 100 ------------------- 150 ------------------- 200
```

[6] INCIDENTEN REPORTED BY

LJ	9 (€ xxx)	SA	6 (€ xxx)
SH	6 (€ xxx)	NB	8 (€ xxx)
WS	11 (€ xxx)		
IY	4 (€ xxx)		