Improving the agility of IT service networks

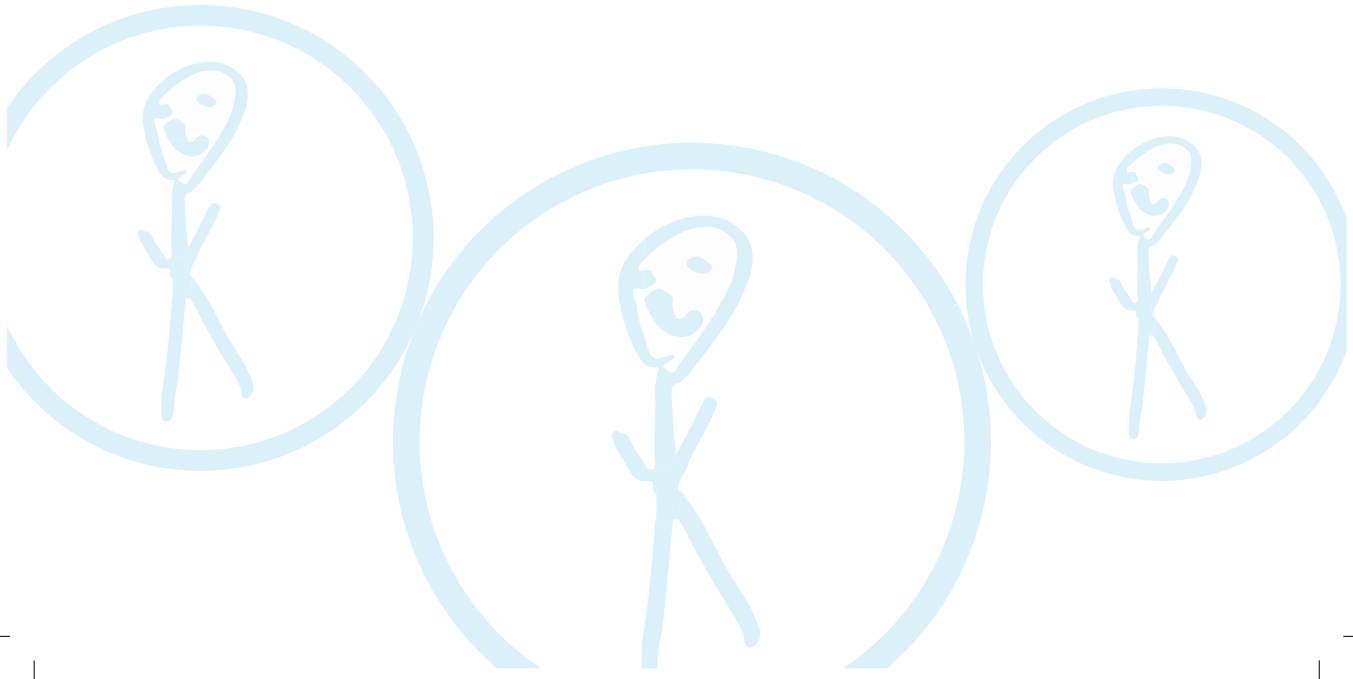
Vlietland, J.J.

2015

document version
Publisher's PDF, also known as Version of record

Chapter 2

Information sharing for effective IT incident resolving in IT service provider networks



CHAPTER 2

Information technology enabled financial services are typically delivered by a network of interdependent IT service providers. Such networks need information to resolve IT incidents in their delivered IT services. The objective of this research is to identify the set of information that needs to be visible within IT provider networks to effectively resolve IT incidents. To this end, we conducted an inductive case study in a network of nine interdependent IT service providers. We found that the required information is distributed over multiple technological stores, and operational IT staff in the network need visibility over these technological stores. Operational staff also needs visibility over the social network of incident handling staff, given the tacit nature of the required information. We therefore premise that better information sharing and enhanced knowledge reuse in the service network has a positive impact on incident handling in IT service provider networks. The main contribution of this chapter is a structured set of information types that positively impacts IT incident handling performance in the IT service network, packaged into a conceptual model.

2.1 Introduction

Business services in large enterprises are enabled by a combination of IT services, delivered by multiple IT service providers. Each of the IT service providers is contractually accountable for one or more IT services (Allen & Chandrashekar, 2000; Niessink, 2001; Susarla, 2003) and uses IT services from other IT service providers, resulting in a network of interdependent IT service providers (Vlietland & van Vliet, 2013). The interdependencies between the IT service providers have a critical nature. A disruption in one of the IT services immediately disrupts the interdependent IT services, resulting in a disrupted overall IT service delivered to the business partner. Failure of such IT service results in failing business services towards clients, potentially leading to extensive financial damage (Oppenheimer, Ganapathi, & Patterson, 2002).

The financial payments industry is a typical example of having such critical interdependencies. A disruption in the payments processor for instance immediately disrupts the payment services of dependent banks (Cheney, Hunt, Jacob, Porter, & Summers, 2012). The critical interdependencies make each of the IT service providers a single-point-of-failure risk in the network of IT services (Nagasubramanian & Rajagopalan, 2012). Next to the delivery of technology an IT service provider acts on events, for instance during IT service disruptions (Bardhan, Demirkan, Kannan, Kauffman, & Sougstad, 2010; Jantti, 2011). Hence, a delivered IT service consists of information technology and additional human activities (Ellram, Tate, & Billington, 2007; Peppard, 2003). The interdependency between IT services results in collaborating IT service staff between IT service providers to jointly resolve disruptions (Jäntti, 2012a; Vlietland & van Vliet, 2013). Effective collaboration is therefore critical to handle IT disruptions and restore the business service swiftly.

We argue that at least two factors obstruct such inter-provider collaboration. First, IT workflow processes are typically implemented on an intra-provider rather than an inter-provider level. This argumentation is grounded in the ITIL literature that targets IT organizations instead of IT service provider networks (OGC, 2007; van Bon et al., 2007). Second, involved staff from different IT service providers typically resides in different locations, disabling face-to-face communication. These two factors introduce collaboration and information sharing impediments, obstructing effective handling of IT disruptions (Shachaf, 2008).

In this study we follow the ITIL standard and define an IT disruption as an IT incident, which is: *"an event which is not part of the standard operation of a service and which causes or may cause disruption to or a reduction in the quality of services and customer productivity"* (OGC, 2007; van Bon et al., 2007). An IT incident that is discovered by IT staff is typically registered in and tracked with an IT Service Management (ITSM)

application. Registered IT incident information in an ITSM application includes an IT incident description, the incident registration timestamp and incident resolving timestamp. The registration and resolving timestamp are used to determine the incident handling duration. ITSM applications also use registered IT incident information to generate aggregated reports about the average realized incident handling performance. IT incident handling performance is typically contractually agreed. An IT incident that occurs needs to be handled within the maximum duration that has been contractually agreed. The term contract in this chapter is considered equivalent to a service level agreement (SLA).

Our prior research targeted the impact of performance information visibility on IT incident handling performance in IT provider network settings (Vlietland & van Vliet, 2013) in which we found that enhancing the visibility of IT incident handling performance by members of an IT service team positively impacts the performance of that team (Vlietland & van Vliet, 2014b).

As that research was limited to enhancing the visibility of performance information, the research question emerged whether other information also positively impacts IT incident handling performance. In this chapter we answer that research question, by identifying the broader set of information that needs to be visible for effective IT incident handling. The research is performed in a case study involving 9 interdependent IT providers in the payment industry.

We found that existing information is scattered over multiple technological and cognitive stores, which results in hardly accessible, highly needed IT incident handling information. In addition, as part of the information has a tacit nature, visibility over the human network supports accessibility to cognitive and (indirectly to) technical stores.

The main contribution of this chapter is a structured set of information types that positively impacts IT incident handling performance in the IT service network, packaged into a conceptual model. That model can be used to improve IT incident handling in IT provider networks and minimize financial damage due to failing business services.

The remainder of this chapter is organized as follows. Section 2.2 explains the used model for the study. Section 2.3 covers related work. Section 2.4 explains the research design used for the case study. Section 2.5 covers our results. Section 2.6 discusses the results, derives propositions from these results and uses a theoretical lens to explain the propositions. Section 2.7 elaborates on the threats to validity and limitations of the research. Section 2.8 concludes the research, deduces the implications and suggests future research avenues.

2.2 Model building

In this paragraph we build the conceptual model that is used as foundation for the research design. The conceptual model is based on control theory. Our prior research used control theory to theorize the relationship between the contractually based incident handling goal, IT incident handling activities and realized incident handling performance (Vlietland & van Vliet, 2013, 2014b). We found in that research that sharing incident handling performance information within an IT provider positively impacts IT incident handling performance of that IT provider. Control theory consists of three fundamental concepts, as shown in Figure 2. The first concept is goal setting; in our case, the goal is predefined by the contract. The second concept is feedback; in our case feedback of the achieved performance level. The third concept is the function (C) that compares output and input; in our case comparison of actual performance and performance goal. The compared result enables the selection of (adapted) action of involved staff to reach the incident handling goal (Andrei, 2006; Forssell & Powers, 2009).

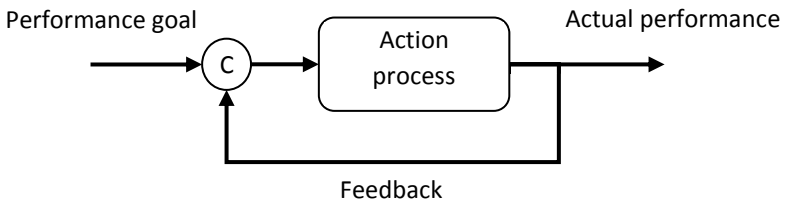


Figure 2, Control theory model

Our prior research used visibility as catalyst for feedback in the control theory model. Visibility of information results in accurate comparison of actual performance and the performance goal. However in that research visibility was limited to performance information (Vlietland & van Vliet, 2014b). In the current research we premise that visibility of other information also enhances incident handling performance (Gregory, Beck, & Carr, 2011) as information is also directly required in the action process next to the performance feedback into the comparison function.

Decision theory, which is related to control theory, uses such a broader view of information to accurately decide on decision making and action taking. Decision theory explains the relationship between action, a set of information and decision making to achieve a set goal (Duffy, 1993; Goodwin & Wright, 2007). A related concept explaining the relationship between information and the action process is the Observe, Orient, Decide Act (OODA) loop of John Boyd (Fadok, 1995). The concept, which is related to

control theory, was originally applied to military operations, using raw information to orient the operation for decision making and action taking.

We premise that the action process in our case requires information from different providers in the IT service network, which is supported by academic work in the IT outsourcing (Blumenberg, Wagner, & Beimborn, 2009; Hamid & Salim, 2011) and supply chain management industry (Rashed et al., 2010; Sahin & Robinson, 2005).

In the sequel, the term 'tiers' is used to indicate the distance in terms of the number of edges between IT providers (Caridi et al., 2010a). A first tier relationship indicates a direct interdependency (edge) between two IT providers (nodes). A second tier relationship indicates two IT providers that are connected via an intermediate IT provider. Hence, the tier level indicates the minimum number of edges that information has to travel between two nodes. Certain information might be needed from the zero-tier, which is the IT provider that takes incident handling action. Other information might be needed from first tier, which are directly connected IT providers. Information might also be needed from the second tier, which is an IT provider that delivers IT services to a first tier IT service provider.

Figure 3 shows the resulting conceptual model. Zero, first and second tier information is required in the incident handing action process. The feedback loop is not included in the model as feedback and the comparison function of control theory are applicable to performance information only.

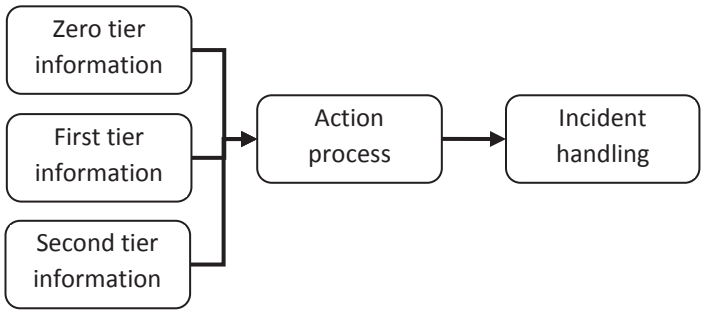


Figure 3, Information – action – performance model

2.3 Related work

A search for related work on information required to effectively resolve incidents in IT provider networks revealed that academic literature regarding this research area is scant. We found and discuss the closest three related research areas: (1) IT service management frameworks, (2) IT sourcing and (3) service supply chain management.

The service operation cluster of the IT Infrastructure Library (ITIL) version 3 framework includes the IT process incident management. ITIL incident management covers identification, prioritization, investigation and solving incidents to restore an IT service (OGC, 2007; Talk, 2013). ITIL Incident management specifies the following information items: incident management rules, incident reports, incident prioritization guidelines, escalation information, incident details and incident status information (Jäntti, 2012a; OGC, 2007; Talk, 2013; van Bon et al., 2007). The related ITIL process service level management refers to the information items: service level agreements, service level reports and existing (infrastructural) IT configuration. A related framework is the Control Objectives for Information and related Technology (Cobit) framework. Cobit targets first line incident management and to a limited extent second and third line support (ITGI, 2007). The covered activities are registering, communicating, dispatching and analyzing incidents of service desks. Both ITIL and Cobit use an intra-provider, not an inter-provider perspective, which is insufficient to extract a reliable set of information items for inter-provider constellations.

An inter-provider perspective is used in the sourcing area although the perspective is limited to dyadic relationships. We did not find any academic literature in the sourcing research area that uses a network perspective. Blumenberg et al. (2009) studied knowledge transfer processes in IT outsourcing relationships, in which their dyadic oriented research mentions the information items: formalized procedures, rules, contracts, SLAs and technical terms. Savić (2008) covered IT incidents in operational outsourcing constellations, although the paper does not include information items that impact IT incident risks. Bartolini et al. (2006) of the Hewlett Packard research lab conducted IT incident handling research, though no information to be shared in service networks is mentioned. The sourcing literature seems not to provide a set of shared information items for IT incident handling within IT provider networks.

The third area we studied is the service supply chain research area. Service supply chains (SSC) also require collaboration and therefore information sharing between providers. The SSC perspective was popularized by Ellram et al. (2004). In their paper they compare the applicability of supply chain models in the services area; however the IT service industry is not covered in their research. Other literature in the service supply chain area does not cover IT provider networks either, let alone a specification of the required information to be shared. One close non-IT match is the paper of Zailani and Kumar (2011), which reports a literature study on service supply chain information flows. The paper mentions the attributes customer request and service planning, however are not necessarily attributes for IT incidents and operational IT plans. We therefore conclude that literature in the service supply chain area does also not answer the main research question.

2.4 Research design

We performed qualitative (Saunders et al., 2009) case study research (Dul & Hak, 2012) at a multinational financial service provider and its supplying IT organizations to gain an in-depth understanding of the used and needed information and get our main research question answered. We developed the following set of research questions for our study:

- What are the IT providers in the selected IT provider network?
- What are the stakeholders in the selected IT provider network?
- Which of these stakeholder roles are highly involved in daily incident handling?
- Which typical incident handling activities are performed by these roles?
- What types of information is shared and/or required by these roles to perform these activities?
- What information is shared and/or required by each of these roles?
- What information is shared and/or required on a first and/or second tier level?

The used research design is based on Eisenhardt (1989), split into two stages as shown in Figure 4. Stage A targets the IT provider network and role mapping, laying the foundation for stage B, that aimed to identify the used and needed information.

The research starts with case selection (step 1), in which we selected a single direct debit card transaction performed by a customer in a domestic retail shop. The scenario requires instant data processing from multiple IT providers. Each of the provided IT services is critically important for successful payment processing (TFSC, 2011). The interdependent IT providers are identified in step 2, by studying archival records and conducting semi-structured interviews at IT providers of the network (Myers & Newman, 2007). The prepared open-ended questions are used to guide the interviews (see stage A questions in the appendix). The interviews are annotated in an interview log and audio recorded for verification purposes. Next to these interviews we use supplementary interviews with candidates working in the IT provider network to collect the information via a snowballing technique. The criteria to participate in the interviews are: (1) having a role in the IT provider network, (2) having information about others in the network, (3) being recommended as interviewee by a manager in the hierarchical structure, (3) being an author of an applicable document (e.g. SLA) and/or being part of the hierarchical structure. The interviews are annotated in interview logs. In addition a data collection log is used to record the activities, the time stamp and the results.

The interview recordings, interview logs, data collection logs and archival records are used to answer the open-ended questions of stage A, shown in the appendix. Using both archival records and semi-structured interviews enables data triangulation (step

3). The network is subsequently mapped in step 4, based on the found interdependencies. Steps 2 till 4 are repeated until all existing interdependent IT providers are included. The involved IT service operation roles are mapped in step 5. Multiple roles are used to enable within-case data analysis. Subject matter experts working in the network are consulted to increase the validity of the mapped network and mapped roles (Gibbert & Ruigrok, 2010).

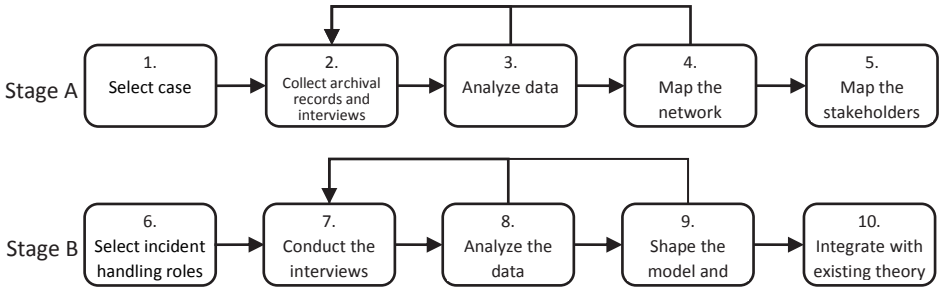


Figure 4, Research design

In the first step of stage B (step 6) the highly involved IT incident handling roles are selected and subsequently interviewed in step 7. Prepared open-ended questions are used to guide the interviews, as shown in stage B of the appendix. The interviews are digitally recorded for content- and construct validity purposes (Mentzer & Flint, 1997). Each interview is analyzed before the next interview, which allows adaptation of the interview script for successive interviews. The iterative approach mitigates the potential problems of Myers and Newman (2007), although the changes in the script were limited.

The setup of all interviews is based on the dramaturgical model, using the metaphor of a theatre to explore social life (Myers & Newman, 2007). The dramaturgical model is based on the general theory of Goffman (1959) that sees social interactions as a drama, with actors that perform in a variety of settings using a script that guides behavior. Both the interviewer and the interviewee play an acting role. The researcher plays the part of an interesting interviewer, the interviewee the part of a knowledgeable person. During the interview a delicate balance is kept between providing direction and getting unbiased answers. Table 4 shows the potential problems of interviews as summarized by Myers and Newman (2007) and our mitigations. The objectives and topics of the interview are set at the beginning of the interview.

Table 4, Potential problems during interviews

Potential problem	Mitigation
Artificiality of the interview	Approach the interview as an interesting conversation. Use a limited structured approach and move gently back to the topic if required.
Lack of trust	Communicate the background of the research, the benefits for the interviewee and the confidentiality of the interview results.
Level of entry	Prepare the interviews by first gaining sufficient knowledge and insight during stage A of the empirical study.
Elite bias	Map the network and the involved roles to ensure that the right IT staff is selected for the interviews.
Constructing knowledge	Triangulate the analysis with archival records, include verifying questions, validate the results with subject matter experts and code one of the transcriptions with a peer.
Ambiguity of language	Include verification questions to verify the interpretation of the used terminology. Mirror by using the words and phrases of interviewees.

The interview results are analyzed in step 8 by transcribing the recorded data. Qualitative analysis techniques are used to analyze the transcripted data (Dul & Hak, 2012; Yin 2009). The qualitative analysis starts with identifying and tagging quotes in the transcriptions (Saunders et al., 2009). The quotes are identified by looking for words and phrases that answer the open-ended questions. The quotes are subsequently tagged with open codes. The open coding process is iteratively performed (Saldaña, 2012). In case a quote applies to more than one open code all applicable codes are linked to that quote. For instance the quote *'Service level agreements are used to share information between roles'*, is related to the codes *'ServiceLevelAgreement'* and *'InformationServiceLevelAgreement'*. Open coding proceeds line-by-line, and proceeds until patterns emerge. These patterns are formalized by grouping the open codes into categories. The categorizing process is done in three ways. First, codes are grouped by prefixes. For instance all codes which are related to information are grouped by the prefix '*Information*'. Second, codes are grouped in code families. For instance the information related codes needed by an '*Incident Manager*' are placed in the code family '*InformationIncidentManager*'. Third, supercodes, predefined queries to retrieve a set of codes, are created for quotes that are related to more than one code or code family. For instance information that is related to the first tier is labeled *'first tier*' and can thus be queried with a supercode. The coding process of the first two interviews is independently performed by a peer and compared with the results of the researcher to minimize analysis bias.

Data collection continues until a new transcription does not significantly contribute to knowledge and insight (Dul & Hak, 2012). Significantly contributing is quantified by

determining whether an additional interview results in more than 5% new or modified codes, which is in line with Sandelowski (1995) and Marshall (1996).

Axial coding is subsequently performed to verify the relationship between information (the cause) that results into effective action (the consequence). After the axial coding process has been completed the grouped information and action codes are clustered into the main categories. These main categories are then clustered to concepts to detail the conceptual model (Birks & Mills, 2011). All steps of the data analysis are recorded in Atlas TI, a CAQDAS package (Gibbert & Ruigrok, 2010; Saunders et al., 2009).

A quantitative analysis is performed on the number of codes in each information category for first- and second tier information and for each interviewed role (Saunders et al., 2009). The number of codes in the first- and second tier is used as an indication of the importance of sharing that category of information within the first tier and/or second tier staff. The number of codes for each interviewed role is used as an indication of the importance of the information category for that role.

In step 9 the conceptual model is detailed and the propositions are defined. During step 10 academic literature is consulted to compare the propositions with existing theory.

2.5 Results

The result section elucidates the results, including typical quotes that enrich understanding. The section is organized as follows. The network of participating service providers and the existing incident handling roles are discussed in subsection 2.5.1. Subsection 2.5.2 discusses the information that all maintenance engineers involved in daily incident handling and incident managers of the most central service provider use and require from themselves (zero tier) or adjacent service providers (first tier information). In a similar vein, subsection 2.5.3 discusses the second tier information that is used and required in the most central service provider. Subsection 2.5.4 discusses the information storage, retrieval, and transfer processes that support information sharing in the provider network. Finally, subsection 2.5.5 discusses the overall conceptual model.

2.5.1 Overview

We identified three networks: the contractual, the technical and the human network. The contractual network consists of the contractual interdependencies between the IT service providers that deliver the IT services. The technical network consists of the

technical interdependent IT systems, delivered by the service providers. The human network consists of incident handling staff that collaborate and share information. A total of 15 planned interviews and 86 supplementary interviews were conducted to collect the information.

Figure 5 shows the mapped network based on the contractual agreements. The full network consists of nine IT service providers. The business partner of the financial service provider has a contract with an internal IT service provider that in turn has a contract with an internal IT hosting provider. The IT hosting provider uses IT infra services from four external IT providers. The business partner has contracts with three external IT providers. Each contract includes a description of the services, and the maximum duration of IT incidents. The IT providers are categorized in SaaS, Paas and IaaS layers. The arrows illustrate the contractual flow of delivery.

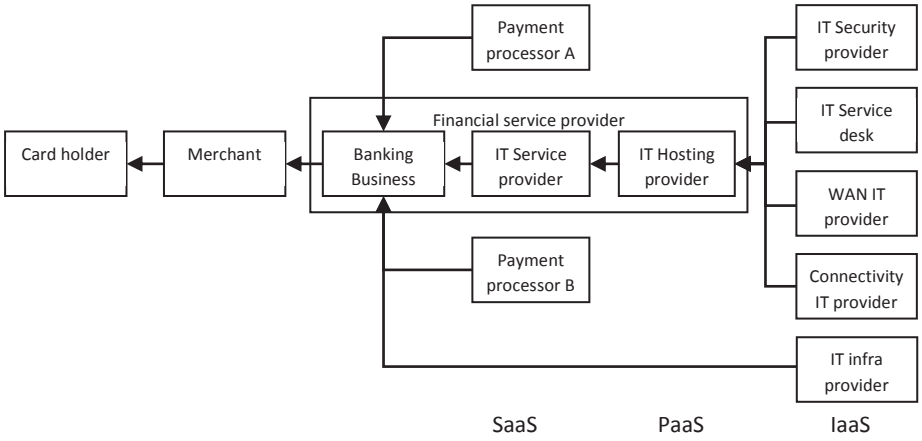


Figure 5, IT provider network map of the research domain

The technical IT network is the second identified network. The technical network is shaped by the technical interdependencies between the IT systems. An electronic payment at a merchants store for instance is sent via the merchant point-of-sales machine to payment processor A, which sends the payment to payment processor B, which sends the payment to the IT service provider. The example shows that the technical information flow differs from the contractual delivery flow (Figure 5).

The third identified network is the human network consisting of collaborating incident handling staff. Each involved member has a defined role in the IT incident handling process, predefined in a standardized role description. The role map in Figure 6 shows five IT service providers, one in each column. Vertically the figure shows for each IT service provider the involved IT incident handling roles, sorted from operational at the

bottom to tactical at the top. Note that the card holder, the merchant, the IT infra provider, Payment processor B, the WAN IT provider and the Connectivity IT Provider are excluded from Figure 6 for simplicity reasons.

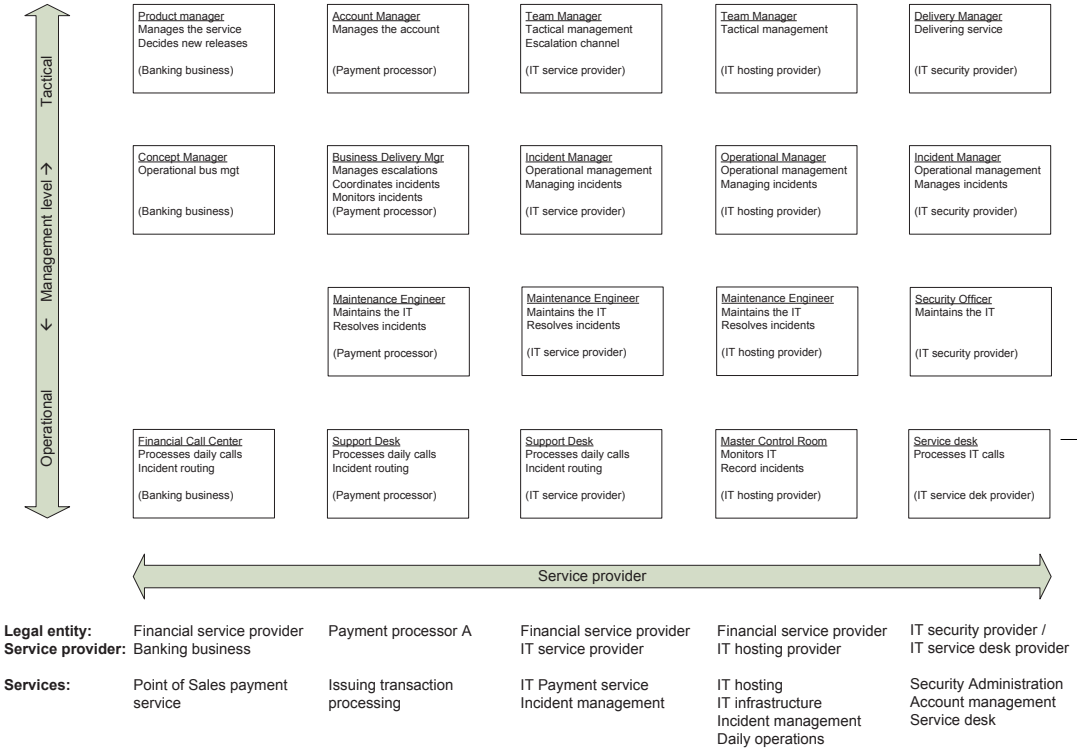


Figure 6, Involved IT service provider roles

Communication between roles varies between IT incidents as each IT incident might occur in different parts of the IT service network, involving different roles and requiring a unique mix of information from different origins. Two incident handling scenarios illustrate possible communication flows that exist during incident handling.

In the first scenario an IT incident is identified by the *Merchant.* The *Merchant* contacts the *Financial Call Center,* positioned at the bottom-left of Figure 6 to report the incident. The *Financial Call* Center subsequently contacts the *Support* Desk of *the Financial Service* provider to report the incident. The *Support Desk* registers the incident in the ITSM application. When the incident gets registered the *Incident Manager* of the *IT service provider* receives a notification of the registered incident through the ITSM application. This triggers the *Incident Manager* to start monitoring the incident handling process. The *Incident Manager* subsequently involves *Maintenance Engineers* from the applicable *IT service providers* to analyze the IT incident. In this scenario the *Maintenance Engineers* discover that payment messages

are not received from the *Payment processor*. The *Support Desk* of the *Payment processor*, handling calls, is subsequently contacted to determine whether the incident is caused by the *Payment Processor*.

In the second scenario the *Master Control Room* of the *IT hosting provider* notices an IT incident via an IT service event monitoring application and registers the incident in the ITSM application. The *Incident Manager* is triggered and involves *Maintenance Engineers* to analyze the incident. As the incident in this case seems to be caused by a malfunction in the security service, the *Incident Manager* contacts the *Operational Manager* of the IT hosting provider. The *Operational Manager* subsequently takes care of incident registration at the *IT security provider,* which triggers the *IT security provider* to start IT incident handling after registering the IT incident in their ITSM application.

Data analysis showed that maintenance engineers and incident managers are highly involved in IT incident handling. Incident managers manage the incident handling process by making sure that all incidents are handled within the contracted service levels. Maintenance engineers analyze and resolve incidents. The incident managers and maintenance engineers roles as shown in Figure 6 were specified in detail by role descriptions based on the ITIL standard.

We interviewed all maintenance engineers and incident managers working in the IT service provider of the financial service provider delivering the selected financial service, since the provider is centrally positioned in the network thus having the largest number of second tier provider dependencies.

Interviews with the incident managers revealed the following typical incident management activities:

- Monitor the duration of open incidents
- Analyze incidents
- Allocate incident to maintenance engineers
- Coordinate incident handling
- Escalate to management in case service levels are at risk
- Distribute daily incident lists including incident handling performance
- Communicate to stakeholders
- Report aggregated incident handling performance

Interviews with the maintenance engineers revealed the following maintenance engineering activities:

- Monitor IT system operation
- Analyze incidents

- Resolve the incident and restore the IT service
- Verifying (sample wise) incident registration quality in the ITSM application
- Maintaining procedures and IT system documentation

The interviews show that the incident handling process is complex, difficult, involves many stakeholders and is frequently time consuming. The following quote illustrates a typical situation during a high priority incident:

> *"I received a phone call that the payments are not being processed. As of that moment you start looking for the cause of the issue. We discovered that the first signs showed up hours before but it takes time to gather everybody. During the subsequent conference call with all involved IT departments and incident managers we were unable to determine the cause, however by reasons that are not known the payments process was restored a few hours later. We later found an error code in a log file although we have not been able to find the root cause".*

For high priority incidents a temporary unique task force with subject matter experts is assembled to resolve the IT incident. The task force is unique as each incident involves different subject matter experts, depending on the nature of the incident.

2.5.2 Required zero- and first-tier information for incident handling activities

This subsection presents the qualitative overview of zero and first tier information, used or needed by incident managers and maintenance engineers. The next subsection presents the qualitative overview of second tier information.

The presented overviews are sorted in the information type contractual, technical and human. Within each type the information is presented from highest to lowest importance, based on the number of quotes (see Table 5). Information categories that are not considered necessary are not covered in the two subsections. First tier information that needs to be visible on a second tier level as well is covered in the next subsection and therefore not covered in this subsection.

The quotes in this subsection and the next subsection are tagged with the information categories from the conceptual model in Figure 7 to support understanding of the result section. Information categories tagged with '(-)' are perceived as missing information.

C3: IT Service level (-)
Contractually based IT incident information is typically stored in the ITSM application and used to track the performance of the incident handling process against the agreed service levels. Registered IT incident information is often insufficient for the incident manager to analyze the incident. Incident managers lack proper understanding of the business impact of the incident, requiring incident managers to collect information from maintenance engineers to determine the contractual impact:

> *Q1: "Maintenance engineers are for me the source to determine the priority",* incident manager
> *"We often need to align with others to determine what is exactly going on",* incident manager

IT service specifications, which are part of the service catalog, are used as benchmark to compare the actual performance with the specified contractually agreed performance.

> *Q2: "What are the parameters of the technical service, what is the uptime of the service and what are the performance agreements of the service. For instance how many transactions should the service process and what is the response time of the service?",* incident manager

T5: Design of IT system (-)
Besides technical information stored in the ITSM application technical information is also used from other stores, to determine for instance which hardware and/or software components are affected by the incident. The interviews show that such information is often perceived as outdated and conflicting:

> *Q3: "Documentation often gets outdated and as a result useless within 6 months. Moreover it is hardly possible to get the latest version of documents, as we usually work with documents that have been delivered by projects and are ineffectively versioned. Documented information in such state is very annoying during incident analysis activities in the middle of the night",* maintenance engineer

System logs are also a technical source of information to determine the root cause of incidents. Maintenance engineers express their need to analyze production logs, while they have no access to such production information. Their need transcends the own IT provider, as maintenance engineers also express their need to have access to logs of interdependent IT providers:

Q4: "We do not have access to production data that would really help to analyze incidents. Sometimes we receive complaints that have roamed around for hours because nobody sees the relationships between de symptoms", maintenance engineer

2.5.3 Required second tier information for incident handling activities

This subsection presents the qualitative view of second tier information that is used or needed by incident managers and maintenance engineers. The presented overview is categorized in technical, human and contractual information. The subsection ends with change related information from a cross sectional network perspective.

C1: Incident in IT service (-)
Incident managers in particular perceive a need for sharing contractually based IT incident management information throughout the chain, while the ITSM application lacks possibilities for sharing such incident related information between IT providers:

Q5: "Before the IT security provider is allowed to spent time on handling the IT incident the IT security provider needs to duplicate the IT incident in their ITSM application. However such duplication is hard as information gets lost over the involved links in the chain", incident manager

Q6: "Our supplying IT service provider uses a different ITSM application that is connected via an interface. This interface is error-prone. To route incidents without errors we need to fill out our ITSM application in a very specific way. The service desk is the only party which is able to do that", incident manager

Incident managers expressed that determining business (end user) impact of an incident against the contract is also problematic, which causes misjudgments during impact analysis, as shown by the following quote:

Q7: "Maybe the internal business partner is also not aware of the severity as potentially 10.000 banking customers can be impacted but only 100 customers have performed this specific action", incident manager

C2: Network of IT services (-)
Information about (the overview of) the technical network and their position in the network is needed by both incident managers and maintenance engineers, to be able to interpret an incident:

Q8: "A maintenance engineer should understand the network and his position in the network… the bigger picture… which suppliers are involved. Such overview

helps to understand incidents as not everything is an incident", incident manager

T1: Technical system process (-)
On an intra-provider level service monitoring applications are used to monitor the service performance of the service provider. As monitoring is restricted to intra-provider level maintenance engineers expressed their need for having inter-provider overview monitoring capabilities over all components:

Q9: "We monitor the IT services very closely. Continuously inspecting the monitoring screens and respond immediately if something weird happens", maintenance engineer

T2: Change in a critical IT system (-)
The cross sectional view on changes in the networks showed that particular IT change related information is considered essential in reducing IT incidents: interviewees stated that 75 - 90% of the incidents are caused by technical changes. Having an overview over all planned and deployed technical changes in the network enables staff to determine incident causes and impact. Both incident manager and maintenance engineer expressed their need for visibility over all technical changes in the network:

Q10: "Often we know what is going to happen within our own organization, but not what is happening at interdependent IT service providers. I am totally unaware what is happening at most of the infra providers, for instance. It would really help to have access to their IT change calendars, to understand their planned changes for the coming weekend", incident manager

Details about IT changes including test results is considered essential information to determine planned IT change impact and consequential IT incidents. Such missing information disables providers to prepare for possible incidents and proper decision making about IT change deployment in production:

Q11: "We would like to have a proper view over what has been tested and whether our acceptance criteria have been met. Under commercial pressure management often decides to deploy changes into production while nobody has a proper overview over the consequences", incident manager

T3: Change in technical capacity (-)
Also unexpected change of payment transaction load leads to IT incidents, which can be prevented in case such information is known upfront:

Q12: "Product management releases a product to a new market segment. Obviously such change has consequences for the capacity of the system. I consider it important that we know what the impact is of such change", incident manager

T4: Network of IT systems (-)
Only high-level technical configuration-items are registered in the ITSM application and the ITSM application is accessible only within the IT service provider. Interviewees therefore perceive a lack of relation understanding between the IT systems and IT components in the technical network:

Q13: "We need to know where a transaction starts and ends, and which interfaces & systems are used. With such information we are able to determine the affected groups during an incident. Information about the technical network is very important", maintenance engineer

H1: Network of human resources (-)
The human network is formed by collaborating staff in the involved IT service providers. The network is utilized for information exchange during incident handling. Accurate contact information is required by incident handling staff for collaboration purposes. Interviewees repeatedly expressed that information about whom and when to contact is lacking, impeding incident handling:

Q14: "It took us more than one and a half day to understand that the point-of-sales machines were causing the issue. At that time we did not have direct access to staff at the payment processor. After we finally discovered who we needed to contact and we contacted that person the problem was solved in no-time", maintenance engineer

H2: Contact details of resources (-)
Contact information includes contact details, such as phone numbers, which is typically missing, as shown in the quote below:

Q15: "Most important is that I can contact you directly to solve the incident instead of getting to you via three points of contact. Next time I would like to call you directly, especially during a priority 1 incident", incident manager

H3: Changes in resources (-)
Also staff changes are considered important information as such information helps to adapt the human network, for instance by communicating the changed contact list, while such information is considered missing:

Q16: "Suddenly we have somebody on the phone that does not even understand which screen to select. Normally we get person x, y or z who knows exactly what we are talking about. However x, y or z are unexpectedly replaced by somebody that lacks knowledge and context, which is obviously less efficient", incident manager

2.5.4 Information storage, retrieval and transfer

Data analysis revealed a various mix of cognitive and technological information stores that are used for incident handling. The technological stores are typically accessible within the IT service provider. Information between providers is almost only shared by means of ad-hoc conference calls, mails and telephone calls during the incident handling process. Documented information that is shared between providers is typically hard to understand, as the information lacks context sharing which is required to properly interpret information:

Q17: "We all should be able to access the same information. However a mainframe document is unusable in a Windows environment… completely unreadable… a different world. Same is true for a Unix environment. So every provider must be able to interpret the information", maintenance engineer

The large amount and dynamic nature of information exceeds the cognitive capacity of the individuals, which brings a need for information sharing and collaboration during incident handling. To quickly access information staff relies on their mental directory of cognitive and technological sources:

Q18: "That implies that I have to know where I need to get my information, which service teams do I need to contact and which systems are maintained. That is why contact information is so important. You need to know where to get the information. That is the most important to me. I expect that my information sources have that information", incident manager

Such interpersonal information dependency has multiple information loss challenges. The information enquiry must be correctly understood by the requestor (staff member 1) and correctly articulated to the provider (staff member 2). The provider has to subsequently correctly understand the enquiry and collect the correct information. The information has then to be correctly communicated and correctly interpreted by the requestor.

Q19: "The essence is that we have access to the information sources ourselves. For example we request information from another IT service provider because we do not have access ourselves. However what we get back is 'yes it looks

good', while we need to exactly know what the other sees on his screen and how fast this is shown. Incidents often take longer because of the lack of information sharing", maintenance engineer

Also the information selection process might be flawed. The following quote shows a business partner that receives a notification from an IT supplier that plans to change the format of data delivery. Since the notification is not correctly interpreted and therefore not passed to the IT service provider, time to process the necessary changes in the IT system is lost, ultimately leading to a major IT incident:

Q20: "Suddenly we did not receive the transactions and our business partner escalated to us that the system was malfunctioning. We started to analyze the incident but were unable not find the root cause. So we sent a mail to the supplier and registered an incident but did not receive any response. After we started calling it turned out that a letter was sent months before to our business partner. However since the business did not understand the importance of the letter we did not take action. When we finally received the letter it notified us that the message format would change and that the receiving IT system should change their message format", incident manager

Also organizational proxies between IT providers impedes effective communication between IT service providers, as additional communication links are introduced and proxies are often unaware of the (technical) context:.

Q21: "The infra supplier are a difficult world to reach. For instance we get information about a malfunctioning of a firewall in a very late stage. The infra provider never notifies such incidents. We also do not have direct access, so telephone calls need to be rerouted to reach them. A very tricky world" maintenance engineer

2.5.5 Conceptual model

The coding clustering process resulted in the identification of three interrelated networks. The first identified network is structured by the contractually agreed IT services, as shown in Figure 5. Visibility over the contractual network is needed to understand the big picture and the position of the IT service in the provider network. The second network is structured by the interrelated technological systems and components that exchange data. Visibility over the technical network is needed for the IT incident analysis process. The third network is the network of incident handling staff, consisting of incident managers and maintenance engineers. Visibility over the human network enables effective collaboration and information sharing.

Table 5 shows for each information category the number of found quotes. The number of first tier quotes for each category is shown in column 2 and for the second tier in column 4, the number of quotes by maintenance engineers is shown in column 6 and for incident managers in column 7. Column 3 shows the % of total first tier quotes for each first tier information category and column 5 the % of total second quotes for each second tier information category. The categories can be either static or dynamic: static information entails the current state of the contracts, technology and human network, dynamic information concerns changes in service levels, service specifications, technology and staff.

Each of the found information categories is clustered into the human, contractual and technical information concept, which is used to build the conceptual model, as shown in Figure 7. The figure shows for the incident manager and maintenance engineer role the dependency on the information categories; the number in each relationship indicates the dependency based on the number of quotes. Information categories tagged with '2' are used or needed by second tier IT providers, information categories tagged with '(-)' are perceived as missing.

Table 5, Number of quotes per information category

Row Labels	1e tier	1e tier %	2e tier	2e tier %	ME Quote	IM Quote
Human	37	14%	38	39%	38	37
Network of human resources	5	2%	26	27%	15	16
Contact details of resources	17	7%	10	10%	13	14
Change in resources	3	1%	2	2%	0	5
Human process	9	3%	0	0%	9	0
Human role	3	1%	0	0%	1	2
Contractual	96	37%	26	27%	59	63
Incident in IT service	54	21%	15	15%	27	42
Network of IT services	15	6%	8	8%	13	10
IT service level	24	9%	3	3%	16	11
Change in supplier service	3	1%	0	0%	3	0
Technical	126	49%	33	34%	98	61
Technical system process	34	13%	9	9%	33	10
Change in a critical IT system	41	16%	9	9%	19	31
Change in technical capacity	20	8%	7	7%	20	7
Network of IT systems	13	5%	6	6%	13	6
Design of the IT system	18	7%	2	2%	13	7
Grand Total	259	100%	97	100%	195	161

1e tier = first tier quotes; 2e tier = second tier quotes; ME = Maintenance Engineer; IM = Incident Manager

Figure 7 shows that maintenance engineers are most dependent on the technical network. Technical system processes are monitored on an intra-provider level, while there is a visibility need over the full network. We also found a need for inter-provider visibility over the network of the codependent IT systems, while such information is currently limited to an intra-provider level. Improved inter-provider visibility over the technical network will likely improve incident handling. In addition, as most of the incidents are caused by IT changes, technical change related information needs to be shared on an inter-provider level. Given the findings in this study we propose:

> *Proposition 1: Technical network information known to incident managers and maintenance engineers in the IT provider network positively impacts IT incident handling performance.*

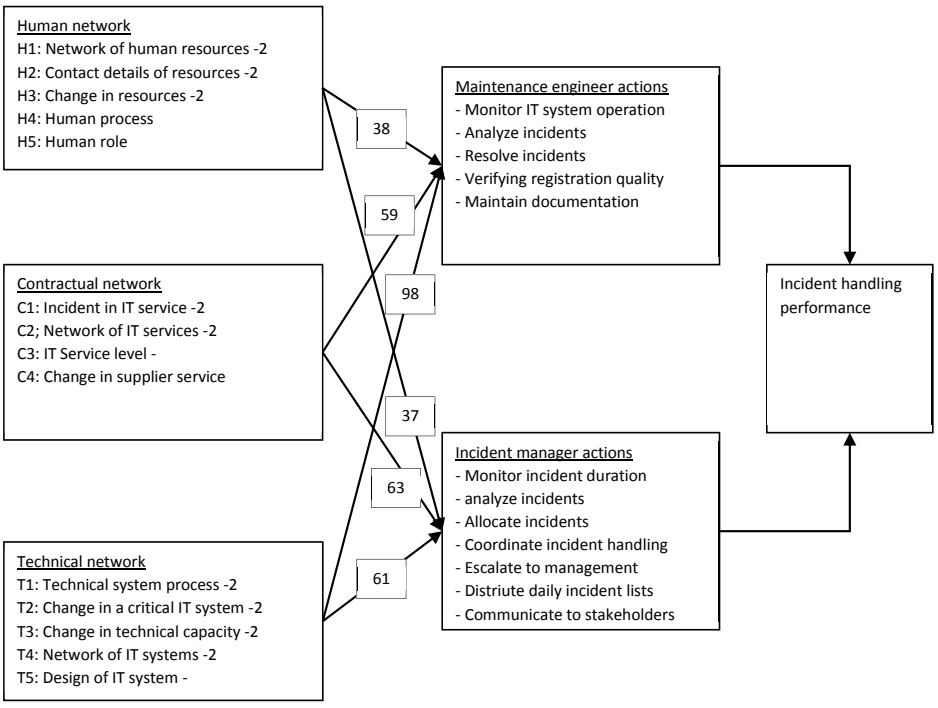


Figure 7, Conceptual model

Regarding the human network, both roles have a need for visibility over (1) the existing network of interacting incident handling staff, (2) contact details about whom to contact and (3) information about staff changes. Interviewees do not perceive a lack of visibility over the IT(IL) roles and IT(IL) processes. Incident handling staff rather has contact details about staff. Moreover we found that the human network acts as an

information sharing mechanism, next to the existing technological stores. We therefore propose:

> *Proposition 2: Human network information known to incident managers and maintenance engineers in the IT provider network positively impacts IT incident handling performance*

IT incident information is considered the most important information in the contractual network, while this is often lacking (Q7) and bound to an intra-provider level (Q5 and Q6). Interviewees also express a need for overview over the network of IT providers to understand their position in the network (Q8). Based on these findings we propose:

> *Proposition 3: Contractual network information known to incident managers and maintenance engineers in the IT provider network positively impacts IT incident handling performance*

2.6 Discussion

This section uses a theoretical lens on the built conceptual model and the three propositions. Technical Information is cognitively and technologically stored and accessed by IT incident handling staff in the network. Accessibility to such stores requires a strong social network that empowers knowledge sharing. The knowledge management research area is related to these findings. Several knowledge management studies support the importance of information sharing in provider networks (Mesmer-Magnus & DeChurch, 2009; Rashed et al., 2010; Vlietland & van Vliet, 2013). Even though Rowley (2007) distinguishes information from knowledge by defining knowledge as information that is processed, transformed and/or enriched, we use both terms interchangeably in the sequel of this chapter.

Knowledge management studies the identification, creation, representation, distribution and retrieval of information (Nonaka & Takeuchi, 1995). Nonaka and Takeuchi (1995) identify two very different types of knowledge. At one end of the spectrum there is explicit knowledge being formal and systematic that is easily retrieved, transferred and stored in technological stores. We follow Frické (2009) and define such explicit knowledge as information as it can be easily stored. Tacit knowledge at the other end of the spectrum is highly personal knowledge, hard to formalize and consequently difficult to share. Business context of the IT provider for instance is hard to transfer between IT providers, while such context supports correct interpretation of shared information, as shown by the quotes Q1, Q4, Q7, Q8, Q13,

Q17 and Q19. The lack of such knowledge can result in incorrect decision making (e.g. Q11, Q20).

We identified two major impediments for information sharing via technological stores. First, technologically stored information is typically bounded to an intra-provider level (e.g. Q6, Q14, Q15, Q21). Second, changes in the network decrease the reliability of technological stored information (e.g. Q3, Q10, Q12). Third, as discussed above, information might be incorrectly interpreted due to lack of contextual knowledge (e.g. Q7, Q17). Staff working in different IT service providers mitigates these impediments with verbal information sharing. The dependency on verbal information sharing implies that staff needs to know whom to contact and how to contact, explaining the importance of the human network (Huysman & De Wit, 2004).

One of the philosophical theories that fits our findings is Transactive Memory Systems (Nevo & Wand, 2005). Transactive Memory System (TMS) theory was first published by Wegner et al. (1991) who researched closed relationships in married couples. A TMS is a collective cognitive store in a group of staff that consists of (1) subject matter information and (2) an information directory of the information stored in the group (Wegner, 1987). The information directory consists of metadata such as people, systems, location, availability, accessibility, reliability and subject matter information (Hamid & Salim, 2011). Incident handling staff has a directory that points to both cognitive and technological stores.

Information directories require less storage than the actual information, thus are easier to encode, store and retrieve, while the member still has access to the information. The downside of information directories is the dependency on information sources (e.g. Q5, Q15, Q16, Q18, Q21); such as cognitive stored information in a staff member that is on leave. This can result in significant information gaps that obstruct incident handling (Q19). Second order information solely based on cognition has the highest chance of such obstruction as multiple linked cognitive stores are involved.

Bug fixing is another area that provides valuable insights. Like incident handling bug fixing (Guo, Zimmermann, Nagappan, & Murphy, 2011) depends on technically and cognitively stored information (Aranda & Venolia, 2009). Tools have been developed to support the human networks in sharing their knowledge. Distributed software development for instance uses tools to bridge the physical distance between software developers (Schuler & Zimmermann, 2008). The tools enhance visibility over the bug fixing process and code changes, which helps developers in their bug fixing endeavor (Begel & DeLine, 2009; Minto & Murphy, 2007). Such boundary spanning technology can also be used to support incident handling. One notable tool is Codebook that

discovers transitive relationships between people, code, bugs and other related artifacts (Begel, Khoo, & Zimmermann, 2010). These tools in the bug fixing area might inspire new ways to improve incident handling.

2.7 Threats to validity and research limitations

This section provides the overview of the threats to validity and our mitigations (Dul & Hak, 2012; Golafshani, 2003; Mentzer & Flint, 1997).

The reliability of the research was enhanced by (1) recording the data collection activities in a log, (2) digitally recording and transcribing the interviews, (3) annotating the interviews in additional interview logs, (4) using a CAQDAS package to analyze the collected data, (5) triangulate the results with organizational documental records and (6) utilizing our prior published research about performance and visibility (Vlietland & van Vliet, 2013, 2014b).

The construct validity of the research was increased by validating the data collection results of stage A with subject matter experts, to mitigate the potential pitfalls of Meyers & Newman (2007). Triangulation of archival records and transcriptions was also used to increase construct validity (Saunders et al., 2009). An independent researcher coded one of the interviews which was compared with the researcher that coded all interviews to minimize coding process bias. The validity of the collected and generated content was increased by using an iterative research design that involved subject matter experts throughout the data collection and data analysis process. Collected content and analysis results of stage B were used in successive iterations to validate the performed data analysis.

Internal validity was improved by theoretically rooting the relationship between the information and incident handling concepts. Traceability of the causal relationship between the concepts was qualitatively performed by the hierarchical coding method and quantitative performed by determining the number of overlapping codes.

External validity was enhanced with interviews at multiple IT providers. We also validated whether role descriptions were similar throughout the network. Nevertheless the external validity in this research has limitations. First, we concentrated the interviews at the IT provider with the highest number of second tier dependencies, arguing that incident managers and maintenance engineers working in this central part of the network have the highest need of second tier information. Second, there are other incident related incident handling roles that can have other information needs, such as the support desks. Third, the interviews naturally exclude

information that is not considered relevant or deliberately withheld by the interviewees.

2.8 Conclusion

This study aimed to find information that is shared and needs to be shared within networks of IT providers for effective incident handling. As the academic literature in this area is scant we studied an IT provider network consisting of nine interdependent IT providers in the payment industry. We conducted 15 planned interviews and 86 supplementary interviews in two subsequent stages. With coding techniques we analyzed and clustered the found information in categories. The strength of the relationship between the information categories and two main roles have been quantitatively analyzed. The information categories are clustered to information concepts to build the conceptual model, used to derive three propositions to theorize the impact of information on incident handling performance.

The results show that human contact information enables access to information and knowledge stores required for incident handling. The results show a perceived lack of most found information categories. Staff relies on information directories as alternative for individually stored subject matter information, resembling a transactive memory system. Staff relies on a cognitive information directory that point to cognitive and technological stored information, rather than have all knowledge cognitively stored.

The results of this study can be utilized for enhancing knowledge sharing capabilities in service provider networks. ITSM applications are likely candidates for developing such capabilities as multiple service providers in a network can use a common (SaaS-enabled) ITSM application. A typical functionally might be a graphic representation of the full provider network (Van Der Aalst, Reijers, & Song, 2005; van der Aalst et al., 2007), with (1) designated staff, (2) all involved IT systems and components, (3) a specification of the involved IT services and (4) the planned and processed technological changes. Developing such ITSM capability is a potential future research avenue, aided by development in the bug fixing industry.

Since we found that IT incidents are usually caused by deployed IT changes, a second research avenue might be the application of TMS to prevent such change related incidents. TMS can offer new ways to better analyze the impact and decide how to deploy such changes with minimal impact.

A third research opportunity is the study of the correlation between (1) cognitive and technological stores and (2) the ‘importance’, ‘urgency’ and ‘dynamic nature’ of the

information. This offers knowledge and insight about the natural preference of the type of storage and the possible improvement to improve knowledge sharing.
As the study covered only one IT service network a fourth research avenue is replication of the study in other IT service networks.

2.9 Appendix

Stage A: Mapping the network

Selecting case

The table below shows the pre-defined questions for the first step in the data collection process that aims to understand the environment of the IT service providers.

Question	Argumentation
To what business is the most downstream IT service provider delivering?	To gain understanding about the business and the dependency from the IT service provider.
What IT services are being delivered by the most downstream IT provider?	Predefined services are required to be able to use the IT service perspective and defining the IT chain.
Have the IT services been contractually agreed?	Contractual agreements helps to identify the IT services and the relationship between two IT service providers (Poppo & Zenger, 2002)
What is the geographical location of the IT workers in the IT service provider?	To what extend the IT service providers in the IT chain are working with IT tooling to bridge geographical distance (Shachaf, 2008), e.g. email, SharePoint, HPSM.
How has the IT service provider been structured?	Insight in the organizational structure of the provider as this defines the distribution of roles and responsibilities.

IT provider network mapping

The table below shows the pre-defined questions for the second step in the data collection process that aims to map the full primary IT chain.

Question	Argumentation
Which upstream IT providers are delivering services to the IT service provider?	The list of providers helps to map the IT chain.
To which downstream IT providers is the IT provider delivering?	Verifying the validity of the structure of the IT chain by using the opposite perspective.
What are the financial flows in the IT chain?	The financial flows increases our understanding of the formal structure and accountability of the contracted IT service in the chain.
What are the operational flows in the IT chain?	The operational flows can differ from the contractual flows, such as an outsourced service desk function.
What is the geographical location of each IT worker in the IT service chain?	To what extend the IT service providers in the IT chain are hindered by geographical distance.
Is each IT service provider in the IT chain a separate legal entity?	Verifying to what extent TCE is present (Thouin, Hoffman, & Ford, 2009)
How is each of the IT service providers internally structured?	Insight in the organizational structure of the provider as this defines the distribution of roles and responsibilities.

Roles mapping

These questions help to define the roles to operationally deliver the IT service.

Question	Argumentation
To which IT services do you contribute?	IT services are the anchor of the interview and it verifies whether the interviewee is aware of the delivered IT service
What is your position in the IT chain?	This shows whether the interviewee is aware of the position of the IT service provider in the IT chain and whether the interviewee has understood the provided information.
What are your tasks and responsibilities regarding the IT service?	This makes clear whether the interviewee understands his role in the IT service.
Which other roles can be identified within the IT service provider?	Follow up question to define the roles.

Validation of IT provider network and roles

These questions ensure that the mapped IT provider network and the roles are valid.

Question	Argumentation
Do you recognize this IT service chain?	To confirm that the right suppliers have been involved in the supply chain.
Do you recognize the services?	To confirm that the services are recognized and fit the existing mental framework.
Do you recognize the IT roles / functions?	To confirm that the roles are recognized and can be used for finding the information that needs to be shared.
Which IT-roles with distinct tasks & responsibilities are involved in regular IT service delivery?	This helps to understand the perception of the interviewee about the roles involved in the chain and to verify the completeness of the IT chain.
Which IT-roles with distinct tasks & responsibilities are involved in restoring the <IT service>?	This helps to understand the perception of the interviewee about the roles involved in the chain and to verify the completeness of the IT chain.

Stage B: Answering questions

Introduction at the start of the interview:

- Purpose of the research
- Explain how we define information
- Service chain with the description of each node and service names
- Stakeholder map with roles and functions
- Clearly explain the distinction between daily operations (blue) and incident handling (red).

Part 1: What is the role of the interviewee?

Question	Argumentation
What is your role during daily IT operation?	To verify if our understanding is valid and it also refines our understanding of the position of the interviewee.
Can you give an example of a not working <IT service>?	Providing an example lowers the artificiality of the interview and therefore contributes to mitigate some of the potential pitfalls of Meyers & Newman (2007).
What is your role during handling such disruption from start to end?	To verify if our understanding is valid and it also refines our understanding of the position of the interviewee.

Part 2: Which information is important for high-performing IT service networks?

Question	Argumentation
Which information do you need to deliver the <IT service>?	Provides a view on what information is considered important to deliver the IT service.
What are the sources of that <information>?	This enables us to better understand the current visibility of the interviewee.
Which loss of information would result in more incidents?	Looking at the opposite perspective to see whether the answers correlate with the previous answer.
Which additional information would enable you to deliver a more reliable IT service?	Let the interviewee look at the incident from a fictional higher performance perspective to see which other information is important. This also gives us a first glance on the important >1 tier information.
Where should that <information> come from?	This helps us understanding the required visibility of the interviewee.
Which information do you need to restore the <IT service>?	Provides a view on what information is considered important to deliver the IT service.
What are the sources of that <information>?	This enables us to better understand the current visibility of the interviewee.
Which loss of information would create more of such incidents?	Looking at the opposite perspective to see whether the answers correlate with the previous answer.
Which additional information would help you to solve the incident faster?	Let the interviewee look at the incident from a fictional higher performance perspective to see which other information is important. This also gives us a first glance on the important >1 tier information.
Where should that <information> come from?	This helps us understanding the required visibility of the interviewee.

Part 3: Which information of second tier nodes is important for high-performing IT provider networks?

The following information needs to be shared with the interviewee at the beginning of this stage of the interview:

– Explain the concept of tiers in the IT provider network
– Explain the concept of a second tier node

Question	Argumentation
Can you give an example of information that you uses from second tier nodes during regular IT service delivery?	Providing an example lowers the artificiality of the interview and therefore contributes to mitigate some of the potential pitfalls of Meyers & Newman (2007).
Which information (from tiers that are not directly connected to your tier) do you use during regular IT service delivery?	Collects existing information >1 tier information that is being used by the interviewee
Which other information (from tiers that are not directly linked to your tier) will help to improve the performance during regular IT service delivery?	This inspires the interviewee to look from a fictional higher performance scenario.
Can you give an example of information that you uses from second tier nodes during incident handling?	Providing an example lowers the artificiality of the interview and therefore contributes to mitigate some of the potential pitfalls of Meyers & Newman (2007).
Which information (from tiers that are not directly connected to your tier) do you use during incident handling?	Collects existing information >1 tier information that is being used by the interviewee
Which other information (from tiers that are not directly linked to your tier) will help to improve incident handling of the IT service the most?	This inspires the interviewee to look from a fictional higher performance scenario.