Master Thesis

Estimation of the costs of IS downtime in organisations:

underlying threats, effects and cost factors

Author:	Qin Li
Study program:	Business Administration
Contact information:	q.li-5@student.utwente.nl

FINAL VERSION

November 2016, Enschede

UNIVERSITY OF TWENTE.

General information

Author	Qin Li
Study program	Business Administration School of Management and Governance
Student number	s1202189
E-mail	q.li-5@student.utwente.nl
First supervisor	Prof. Dr. Ir. L.J.M. Nieuwenhuis School of Management and Governance l.j.m.nieuwenhuis@utwente.nl
Second supervisor	Mr. Abhishta School of Management and Governance s.abhishta@utwente.nl

Management summary

Information system (IS) has been widely applied in companies to support sophisticated activities and processes so as to enhance efficiency and reduce costs. The availability and reliability of the IS infrastructure is critical. However, the IS system can be fragile. Once the problem occurs, it will cause both performance and financial losses to the company.

This thesis proposes an IT downtime costs model for all types of organizations to evaluate financial losses in order to know how much money should invest to improve the IS. To find out the costs of downtime, this thesis analyses interdependencies of components, downtime threats, and corresponding effects.

There are 10 main causes threatened the health of IS: *natural disaster*, *hardware failure*, *software failure, and human error, system overload*, *computer virus/hacker attack*, and, *loss of network connectivity*, *power outage*, *vandalism* and *maintenance*.

Literature and interview results show that downtime affects the company in terms of *idle employees and equipment*, *productivity losses*, *data losses*, *reputation damages*, and *customer losses*.

Based on the damages of IS downtime, we find two types of costs: direct and indirect costs. There is a direct link with the *costs of idle employee* and *idle employee and equipment*. Two direct expenses related to the fix of the system: *repair costs* and *compensations for work overtime*. Indirect costs generated from *damaged reputation*, *customer loss*, and *productivity loss of employees and equipment*, are *revenue loss* and *compensations for customers and partners*.

Therefore, the new IS downtime cost model comprises of idle costs of employees, repair costs, compensation costs for work overtime, revenue losses, and liability costs.

Table of Contents

List of figures

List of tables

Abbreviations

1. Introduction

This chapter introduces the topic of this thesis – ***estimating the IS downtime costs***. The *background and problem statement* is addressed from a theoretical context (1.1). The *research motivation* is placed next to this section (1.2). Thereafter, the *research questions* (1.3), followed by *research objectives* (1.4), and *research methods* (1.5). Finally, *thesis structure* is presented (1.6).

1.1 Background and problem statement

As the development of the World Wide Web, the information sharing has become much easier. The capabilities of extracting and processing the useful information are crucial to companies. Once the company can manage the capabilities well, enormous social impacts and benefits can be generated (Zardini, Rossignoli, & Ricciardi, 2016). The cyber-physical system is designed to help companies to connect the cyber-world of computing and communications with the physical world (Rajkumar, Lee, Sha, & Stankovic, 2010). To support the connection between the cyber world and the real world, Information system (IS) infrastructure is the foundation in which all the necessary facilities and services are interconnected to achieve better performance (Jessup & Valacich, 2007). In order to survive and grow in the market, companies devote themselves to develop or apply an appropriate IS infrastructure (Porter & Millar, 1985). With the IS services, companies are highly connecting with each other and involving in networks to share information and communicate (Rinaldi, Peerenboom, & Kelly, 2001). Besides, IS triggers innovation and leads to competitive advantages for a company (Bhatt & Grover, 2005), which has been largely improved companies' critical issues, such as productivity, cycle times, customer service and responsiveness (Chanopas, Krairit, & Khang, 2006). Therefore, many companies have placed the development of an effective IS infrastructure among the top concerns over IS management.

Due to the rapid changes in technology, organizations invest a huge amount of money in IS. They are more and more dependent on information technology, therefore, they are expecting high level availability of IS (Franke, 2012; Gable, Sedera, & Chan, 2008). Byrd and Turner (2000) states that companies on average spent around 58 percent of organizational IS budgets on IS infrastructure and the spending increase 11 percent per year. However, the implementation and operation of IS infrastructure is risky. It may not cooperate with the firm's existing business processes, which can lead to IS downtime (unable to perform designed tasks) (Ramirez, Melville, & Lawler, 2010). IS downtime costs are hard to estimate, because of a multitude of internal and external effects. However, Pascual, Meruane, and Rey (2008) address the importance of estimating downtime costs: 1) it allows to measure system efficiency: 2) by using key performance indicators, the effectiveness of maintenance policies can be measured; 3) the mathematical model provide insights during the decision-making process. According to a survey from Information Technology and Intelligence Corp.,

companies cannot avoid downtime and one out of 10 companies said they need greater than 99.999% availability ("Trends in high availability and fault tolerance," 2010). Two hundred companies from North America and Europe reported that the total loss from IS downtime is over $26.5 billion in one year (Harris, 2011). Yet, the survey does not clearly identify the relationship between the specific downtime causes, their effects, and correlated financial losses. Therefore, this thesis investigates the factors that cause the downtime of IS and proposes a model that can be applied to estimate the costs of downtime. Thus, estimating the downtime costs of IS infrastructure is essential for companies.

1.2 Research motivation

The motivation for this research has come forth out of both huge operational problems and financial impacts to the company and its customers due to IS downtime. When only a portion of the IS infrastructure has failures, the ownership suffers loss (Franke, 2012; Patterson, 2002). For example, in healthcare, IS is involved in every aspect of patient care, from billing to sophisticated image-guided surgery systems (Campbell, Sittig, Guappone, Dykstra, & Ash, 2007). If the IS system breaks down, it results in accounts management delay and can even threaten patients' life. A survey showed that 48.9% of 178 IS related participants put the availability on the top of IS system quality in their company. Another survey from 2010 with CEOs and senior business executives show that IS availability and its costs is put on the second place of concerns (Franke, 2012). Therefore, synthesizing the factors that cause IS downtime is crucial to accurately calculate the downtime costs and methods that minimize the IS downtime costs are valuable to companies to give better performance and financial results.

1.3 Research questions

Yet companies do not establish an efficient and effective model to calculate their IS downtime costs because companies do not fully understand the causes of IT downtime and know little about the measurement of downtime costs. Although researchers have addressed some methods to calculate the IS downtime costs based on the corporate-wide perspective (Patterson, 2002), not all effects have been taken into account. Downtime does not make trouble for direct users but also affects other entities within the network, such as other infrastructures and companies. Failure occurs on one part of the network can generate chain effects on other systems. Therefore, the main research question is: ***How to calculate the downtime costs of IS infrastructure?*** In order to address this question, the following sub-questions are asked:

Sub-question 1: how is the IS infrastructure related to its environment?
Sub-question 2: what are the causes of IS downtime?
Sub-question 3: what are the effects of IS downtime?
Sub-question 4: what are the costs of these IS downtime effects?

1.4 Research objectives

Although there are a number of articles that formulate an empirical model to calculate the costs of downtime, there is nearly no literature addressing the causes of downtime and corresponding costs. The objective of this thesis is to develop a general IS downtime cost model that applies to all companies. To achieve that results, we identify the IS interdependencies of downtime causes and analyse the related costs.

1.5 Research methods

The general method of this research is based on qualitative research. Qualitative research is a mean to explore and understand the drivers of individuals or groups related to a social or human problem (Creswell, 2013). Under this method, specific methods are used - systems modelling and activity-based costing, to category the cost factors.

Based on this method, questions and procedures are developed firstly. Then, data is collected through semi-structured interviews, and collected data is analysed. Results are built from particular to the general case. Survey results from existing paper and other publications are used as extra sources for validating the model. Finally, meaningful interpretations of the data will be made.

To collect information, this thesis uses literature and interviews. The literature review provides the theoretical background, so an initial model can be built. The interview offers more insights to the problem and gives some valuable practical information which shapes the model.

1.6 Thesis structure

The remainder of this thesis consists of seven sections. In Chapter 2, by review existing literature, the notion of IS infrastructure, IS interdependencies and IS downtime are discussed; the causes, reactions, time issues, and the formula of costs of IS downtime are presented as well. After that, the methodology is discussed in Chapter 3. Subsequently, in Chapter 4, we compare whether there are differences between interviews and surveys results and literature. In Chapter 5, based on the results of interviews, the new IS downtime costs model is formulated. And then, the theoretical and managerial implications of the model are pointed out in Chapter 6. In chapter 7, we present out conclusions. Finally, in Chapter 8, we discuss the limitation of this study and suggest interesting topics for future research.

2. Literature review

In this chapter, key concepts are explained and discussed. This section is divided into three sub-sections, starting with the definition of IS infrastructure (2.1.1) and its interdependency (2.1.2), and following by clarifying the causes of IS downtime (2.2.1), types of damages (2.2.2), and reactions to downtime (2.2.3). Associated costs of downtime presents in section 2.3, Due to the fast development nature of IS, the time boundary of articles is set, from 2000 to the year this research conduct - 2016. Articles published before 2000 are considerable, only if it is still cited by recent publications.

2.1 IS infrastructure and its interdependency

This section starts with the definition of IS infrastructure - *"IS infrastructure is a collection of technologies, people, and processes that facilitates large-scale connectivity and effective interoperation of an organization's IS application*" (Kumar, 2004, p. 11)

IS infrastructure is the top concern of IS management and information system executives, due to the fact that IS infrastructure supports the process and capability integrations crossing business and functional units (Broadbent, Weill, Clair, & Kearney, 1999; Byrd & Turner, 2000) and is vital for development time and costs (Duncan, 1995). According to Bharadwaj (2000), IS infrastructure plays an important role in linking the key suppliers and customers through the entire organization, which is a key resource for company's long-term competitive advantages. Therefore, it is necessary to study the IS infrastructure and its relationship with other entities of the organization.

2.1.1 IS infrastructure

To understand IS infrastructure, Hughes and James (2009) explained that the infrastructure runs applications where customer data are processed and handled. Besides, market insights are generated and analytical tools are supported. In this way, it becomes easier for executives and managers make and communicate the decisions shaping a complex organization. Jessup and Valacich (2007) identified seven main components of the IS infrastructure:

- *Hardware*: the hardware is not only computers but also networking hardware. Computing hardware stores and processes organizational data and networking hardware connects different systems to allow for collaboration and information sharing.
- *Software*: software offers supports on executing business processes (utilizing information system hardware and networks) and competitive strategy to create an effective and efficient environment.
- *Communications and collaboration*: with the number of interconnected computers and some other necessary hardware and software, such as e-mail servers, IS infrastructure enables the internal and external communication and collaboration.
- *Data and knowledge*: these are the most important assets that an organization has to gain

business intelligence and execute business processes.

- *Facilities*: this refers to the equipment that does not directly support the business processes or business intelligence, but is necessary for information transfer.
- *Human resources*: this refers to the availability of well-trained employees, who can provide necessary assistances as need.
- *Services*: due to the high costs of maintaining and upgrading hardware and software, IS services is not a part of the core business or even not a part of the business. Instead, companies corporate with outside service providers.

Chanopas et al. (2006) further explained that IS infrastructure is the foundation for both the communication across the organization and the implementation of present/future business applications. This shared communication function makes IS infrastructure different from business application, which serves for future applications and services of all business units (Saaksjarvi, 2000). Valacich and Schneider (2010) view the IS infrastructure as the underlying platform to perform business processes, core processes and supporting processes.

According to Byrd and Turner (2000) and Chanopas et al. (2006), IS infrastructure can be divided into two components: technical IS infrastructure and human IS infrastructure (see Figure 1). The technical infrastructure servers for applications, data, and technology configurations, including hardware, software, the network, telecommunications, and other tangible IS resources. These are the base for shared services between business applications. Valacich and Schneider (2010) considered that data centre as a separate entity of the IS components, since it can be viewed as a sub-infrastructure, where data is stored, transferred and analysed to support the whole IS infrastructure. In this thesis, the data centre is an element that distinguished from IS components. The human IS infrastructure refers to the knowledge and capabilities required to manage effectively the IS resources within the organization processed by IS personnel. According to Saaksjarvi (2000), human IS infrastructure transfers the IS components into useful IS infrastructure service through employees' knowledge, skills, and experience. The unique personal capabilities convert the IS infrastructure as a valuable resource and ensure the uniqueness of IS infrastructure. In addition, IS personals ensure the continuity of the IS, to offer the agreed performance to both employees and customers. When a problem occurs, technicians detect and identify the faults to minimise the effect. Therefore, human IS infrastructure is important and it creates the uniqueness of IS infrastructure for each company, to make it hard to imitate.

Figure 1 shows the general structure of IS infrastructure in organizations. In this thesis, we follow Jessup and Valacich (2007)'s view, which IS infrastructure includes seven sub-infrastructures: hardware, software, communication and collaboration, data and knowledge, facilities, human resources, and services. The relationship of sub-infrastructures will be elaborated in the next section.

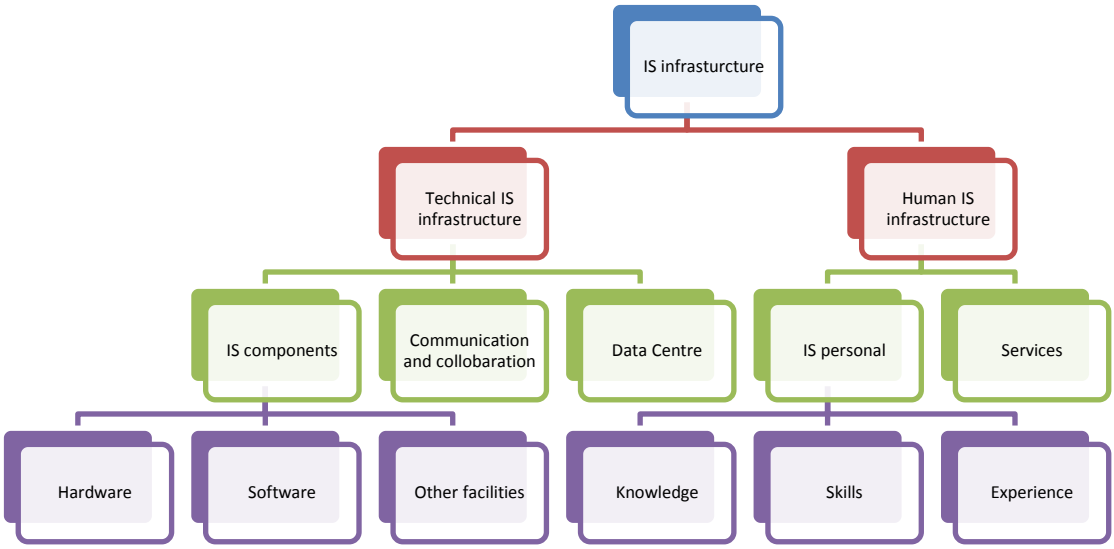

Figure 1: Structures of IS infrastructure

2.1.2 Identifying critical interdependencies of IS infrastructure

Business continuity is vital; however, the complex technological nature of IS infrastructure puts the continuity at risk (Becker, Goldszal, Detal, Gronlund-Jacob, & Epstein, 2015). Finding out the interconnection of components is critical to managing downtime. Infrastructures are usually connected at multiple points through a wide variety of mechanisms, which is called infrastructures interdependency - "a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other." (Rinaldi et al., 2001, p. 14). Rinaldi et al. (2001) proposed four types of interdependencies among global infrastructures: physical, cyber, geographic, and logical interdependency. We study these interdependencies at the level of infrastructures within a company.

- *Physical interdependency*: physical interdependency occurs when there are physical linkages between the inputs and outputs of two entities that the state of each relies on the output of the other (Rinaldi et al., 2001). Although the IS infrastructure itself does not transfer physical goods, it can be the underlying support for logistic companies which deliver goods via IS.
- *Cyber interdependency*: this type of interdependency is based on the information transmitting through the whole information infrastructure, which links via electronic and informational elements (Rinaldi et al., 2001). In a company, a large amount of data is stored in massive amounts of disk space and large internal (RAM) memories to allowing quick access (Friedman, 1998).
- *Geographic interdependency*: geographic interdependency refers to the local natural events can make changes on infrastructure due to the close spatial proximity (Rinaldi et al., 2001).

- *Logical interdependency*: this refers to the linkage within a control scheme that the state of each depends on the state of the other via a mechanism without any direct physical, cyber or geographic connection (Rinaldi et al., 2001).

Treating IS infrastructure as an entity, which can lead to different kinds of interdependencies with its environment. Basically, the IS infrastructure builds on the cyber interdependency, in which hardware and software are connected by cyber connections. The main function of hardware is to store and display information or data. To the contrary, software refers to computer instructions or data (Valacich & Schneider, 2010). It has to be noticed that neither can be realistically used on its own. Therefore, the relationship between hardware and software is based on cyber interdependency. Things connect with humans are based on logical interdependency. Employees put resources into the cyber system that go through the cyber system to deliver the expected function or services to employees. On the top of this, data and knowledge are the valuable intellectual property of the IS and the company. Managing data and knowledge is essential for both gaining business intelligence and executing business processes (Jessup & Valacich, 2007). It requires both reliable system but also appropriate people with necessary knowledge, experience and skills.

The interdependencies of the IS infrastructure components is shown below.

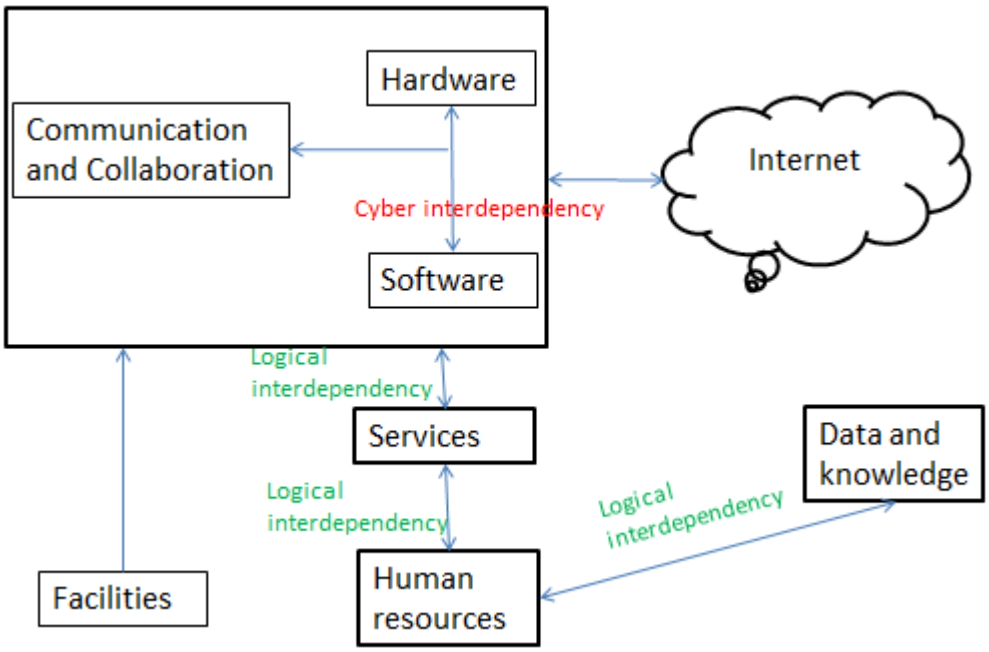

Figure 2: Interdependencies in IS infrastructure

2.2 IS downtime

IS downtime can be caused by many factors. Therefore, we address the causes of downtime firstly (2.2.1). Next, effects of the downtime are shown (2.2.2). After that, we study the reaction to downtime categorise effective solving methods (2.2.3). Time also plays an important role during downtime (2.2.4)

2.2.1 Causes of downtime

The downtime refers to the time that the IS infrastructure provides improper service. Proper service is the behaviour as specified and experienced by the environment of the system. The system fails when the system is not delivering proper service. According to literature, there are two basic measures: reliability and availability (Bosse, Splieth, & Turowski, 2016; Franke, Johnson, & König, 2014; Takezawa, Nakahara, Uenohara, Takayama, & Okuda, 2010; Zambon, Etalle, Wieringa, & Hartel, 2011). Bowen (2013) gives the definition of reliability and availability. "The reliability is a measure of the continuous delivery of proper service. The availability is a measure of the delivery of the proper service with respect to alternation of delivery of proper and improper service." (p.6). These definitions can be related to stochastic variables, which mean that these measures are probabilities. Mean time to failure (MTTF) is the mean time to the failure of the system. If we assume that the system can be repaired after a failure, then we can define the mean time between failures (MTBF). Similarly, we can define the mean time to repair (MTTR), i.e., the average time needed to repair the system after the system failure occurred. Using these measures, the reliability can be expressed by MTBF that MTBF = MTTF + MTTR (Low, 2015). Availability can be defined as $\mathbf{Availability} = \frac{\boldsymbol{MTTF}}{\boldsymbol{MTTF+MTTR}}$ (Franke et al., 2014).

Callaghan and Mariappanadar (2008) distinguished the causes of downtime as planned and unplanned downtime. The unplanned downtime comprises seven categories: acts of nature, hardware, software, and human error by someone inside a company, human error by someone outside a company, system overload and vandalism. In addition, companies are constantly performing planned outage to maintain hardware and software in order to avoid an unplanned outage. This type of outage is controllable both in routine and time. Although more and more companies expect that there is no outage during the planned maintenance, sometimes the temporary outage is inevitable. Lei et al. (2014) added the more causes occurring in the health care, computer virus/hacker attack, loss of network connectivity, electronic power outage and causes unknown or not disclosed.

Regarding the existing literature, the causes of downtime has been categorised as follows:

- *Natural disaster*: earthquake, flood and other natural events can damage the system which is unpredictable.
- *Hardware failure*: this refers to the failure of hardware, such as CPUs and Monitors, which makes the processes lose control of the network and destroys the resources needed for the other processes (Rosen, 1981). According to Becker et al. (2015), hardware downtime accounts for 13% of the downtime causes.
- *Software failure*: software defects means that software applications do not perform the required operations (Callaghan & Mariappanadar, 2008). Becker et al. (2015) also showed that the most common downtime cause is the failure of software, accounting for 73%.
- *Human error (inside or outside the company)*: this refers to the inappropriate actions, such as the omission of events, incorrect data entry, and mischaracterization of the

metrics, made by human beings (Becker et al., 2015).

- *System overload*: this is the situation that a component runs over its capacity reservations in a certain time period (Mercer, Savage, & Tokuda, 1994). In the real-time environment, tasks have different timing constraints and compete for resources (Caccamo, Buttazzo, & Lui, 2000). For example, when a critical component runs much greater than the actual needs which cannot be summarily truncated, this leads to a low efficiency and wastes the available resources (Caccamo et al., 2000; Mercer et al., 1994). Tasks can be stacking in the next step because of the high time variance. The main cause of downtime is that there are insufficient resources to conduct the next step
- *Computer virus/hacker attack*: computer hackers are trying to access the data and disturb the system through various channels, for example, computer virus, damaged the devices and their resources (Saied, Overill, & Radzik, 2016). DDoS (Distributed Denial of Service) is a threat that company faces when connects to World Wide Web (Mehic, Slachta, & Voznak, 2016; Sieklik, Macfarlane, & Buchanan, 2016).
- *Loss of network connectivity*: this refers to the situation that the client computer cannot get any response from the application or server.
- *Power outage*: as for computer hardware system (e.g. computers and servers), it cannot run without electronic supply. Once the electronic power outage happens, all the hardware stops working.
- *Vandalism*: people damage the computer components or systems on purpose. This has to be distinguished with the unconsciously human error.
- *Causes unknown or not disclosed*: this category includes all other causes that are not mentioned above.

2.2.2 Types of damages

Dübendorfer, Wagner, and Plattner (2004) stated that the damages of IS downtime are not only related to the downtime period which can be directly measured in terms of finance, but also other damages after the problems are solved. The researchers identified four types of damages: downtime loss, disaster recovery, liability and customer loss.

- Downtime loss: due to the downtime, employees and the equipment cannot perform the usual tasks that lead to productivity loss. Moreover, if the downtime affects customers' access to the services, the revenue loss occurs.
- Disaster recovery: this includes the time of employees spending and also the purchasing costs on necessary materials on recovery from the disaster
- Liability: if the downtime results in lower level of service that the company promised to their customer on service level agreements (SLAs), customers can ask for a compensation payment. Besides,
- Customer loss: a worse case of degraded service quality made by IS downtime is that customers terminate the contract and less new customers join in.

When downtime happens, a number of employees and equipment is unable to perform tasks. The breakdown causes lower productivity that less revenue is generated. Liability and customer losses lead to financial losses that usually appear some time later after the downtime.

Disaster recovery is a special case that the company suffers the natural incident and the damages may be much more than any other causes.

2.2.3 Reactions to downtime

When downtime occurs on personal desk computer, Becker et al. (2015) suggested to restart the system, otherwise, problems need to be fixed by technical staff. Labib (1998) stated that there are three main phases to react to downtime. The first one is *response phase*, which refers to "the time between the occurrence of a breakdown and the attendance of a maintenance engineer" (p.67). The second phase is *diagnostics phase* where problems are identified and solutions are developed where engineers are distributed into different parts to finding and analysing breakdown. Prasad Nepal and Park (2004) argued that identifying the fault point(s) requires competent mechanical engineering knowledge. Without qualified technical knowledge, it is not efficient in reducing the nonworking period and costs. In this case, the company may hire external experts for help. The last one is *repair phase* that refers to the time taken to solving breakdown problem, where tools and replacing elements are needed for fixing. If the breakdown components are critical to the running of business, the manager may consider renting a system from another company to minimise the idle production (Cronholm, 2000).

The IS infrastructure has the potential to break down, which means that problems exist in the system, but do not happen yet. When the breakdown happens, technicians follow these three steps to repair the system. The time spend on these three phases can be viewed as repair time. If companies can reduce the repair time and keep the MTTF constant, the availability of the system increases. Researchers named this type of action as corrective maintenance or reactive maintenance (Chang, Ni, Bandyopadhyay, Biller, & Xiao, 2007; Cronholm, 2000). On the other hand, corrective maintenance improves the equipment reliability that there are less possibility of equipment failures (I. P. S. Ahuja & Khamba, 2008) because the MTTF increases. Therefore, knowledgeable technicians play an important role in reducing downtime.

Figure 3: Downtime reaction processes

In the study of Becker et al. (2015), the average downtime period is 3.5 hours ranges from less than 1 to 48 hours. The outage time caused software error is usually shorter than which by hardware error. An example showed that the hardware downtime lasts 32 hours (Becker et

al., 2015). Lei et al. (2014) had the similar result that the most common failure occurs in software, 49 times, followed by hardware failure occurs 27 times during the research period. Besides, Harris (2011) reported that companies experience 14 hours of IS downtime annually.

2.3 Costs of downtime

Downtime impacts the company not only in terms of equipment and employees but also financial issues. The first consequence of downtime is the idleness of equipment and employees. Employees report the breakdown and wait for repair. Therefore, the main costs in the response phase and diagnostics phase are the idle costs for equipment and employees. Repair phase incurs repair costs, such as replacing components. In addition, Dübendorfer et al. (2004) believed that the downtime affects the overall productivity. Halligan, Demsetz, Brown, and Pace (1994) defined this productivity as "the reduction in productivity caused by unanticipated conditions" (p.49). In this thesis, loss of productivity comprises idle costs for employee and equipment, since idle employees and equipment directly lead to productivity reduction.

- *Idle costs for equipment*: this category includes the idle costs of broken equipment and its dependent equipment. The equipment is expected to working fully and productively until the end of its service life to cover the investment costs and earn revenues, while downtime stops the equipment to make expected benefits (Prasad Nepal & Park, 2004)
- *Idle costs for employees:* this is the costs associated with the idle time of human resources. The breakdown of equipment causes employees being idle, however, company has to pay wages to the employees even they are idle (Prasad Nepal & Park, 2004)
- *Revenue losses*: this refers to the loss of customer access due to the inability of a company to fulfil customer request (Dübendorfer et al., 2004). The customer service transactions drop during downtime or may be broken.
- *Repair costs*: this refers to the costs that spend on repairing broken components, such as buying substituted components. Besides, companies may rent the necessary equipment from outside if the breakdown affects the critical activities and lasts for a long time (Tsimberdonis & E. Lile Murphree, 1994). The rental fee falls into this category
- *Liability costs:* Tsimberdonis and E. Lile Murphree (1994) defined this concept as the financial loss of important equipment breakdown in contractual obligations and clauses agreed on for the particular project which is invalid and unenforceable. Liquidated damages occur if the company cannot deliver the promised tasks to its contractual partner (Dübendorfer et al., 2004).
- *Disaster recovery costs*: this refers to the money spend on time, material and people recovering from the natural disaster (Dübendorfer et al., 2004).
- *Customer losses*: different customers generate different revenues for the company. When they go to another service provider, the losses incurred. However, it appears some period later if the service unavailable for some time (Dübendorfer et al., 2004).

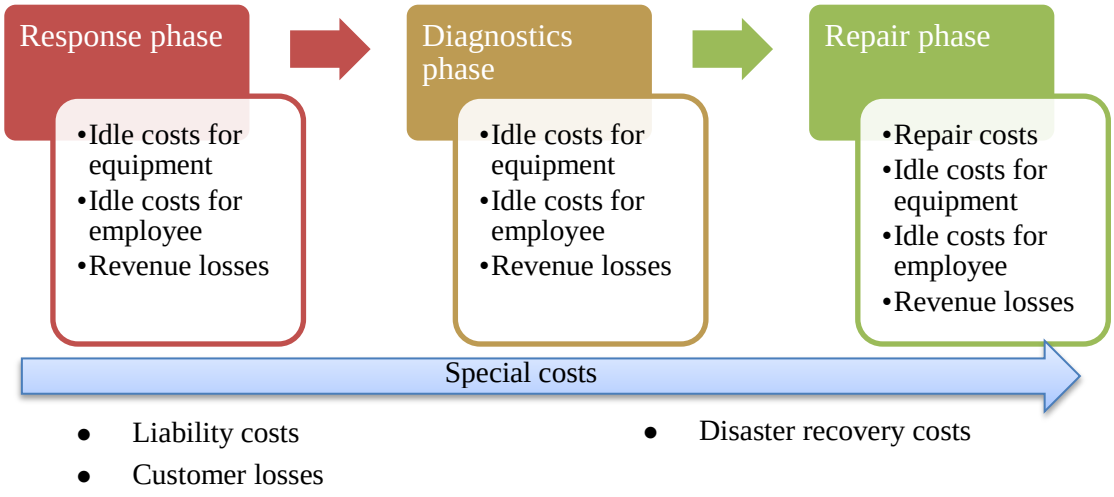

Figure 4: Associated costs of downtime

Based on previous research, in this thesis, there are seven main costs categories related to IS downtime, which is calculated as:

Total downtime Cost = idle costs of employees + idle costs of equipment + revenue losses + repair costs + liability costs + disaster loss + customer loss

Idle costs of employees = $\frac{W_e}{T_e} \times T_i \times N_{ed} \times P_d$

Idle costs of equipment = $\frac{O_{eq}}{T_{eq}} \times T_i \times N_{eqd} \times P_d$

Revenue loss = $\frac{\text{ꙅ}}{T_o} \times T_{od} \times \text{ꙅ}_d$

Repair costs = $C_{bc} + C_e + C_r$

Liability costs = $\sum C_c + \sum C_t$

Disaster loss = $N_{er} \times C_r \times T_{ro} + C_m$

Customer loss = $\left[C_a(\Delta t) + C_p(\Delta t)\right] \times R_c(\Delta t)$

Factor	Symbol	Unit
Idle costs of employees and equipment		
Employees' wages per year	W_e	€/yr[1]
Working time per employee per year	T_e	h/yr
Number of employees affected by downtime	N_{ed}	
Equipment's annual throughput	O_{eq}	
Working time per equipment per year	T_{eq}	h/yr
Number of equipment affected by downtime	N_{eqd}	
Productivity degradation during downtime	(P_d)	
Idle time during downtime	T_i	
Revenue loss		
Total annual revenue	⍉	€/yr
Service operating hours per year	T_o	h
Service operation time affected by downtime	T_{od}	h
Part of the revenue affected by downtime	⍉$_d$	
Repair costs		
Costs for replacing components	C_{bc}	€
Costs for hiring experts	C_e	€
Costs for renting equipment	C_r	€
Liability costs		
Claims from contractual penalties	C_c	€
Claims from other liabilities	C_t	€
Disaster loss		
Number of employees in the recovery team	N_{er}	
Costs per hour for a recovery team member	C_r	€
Recovery work hours outside office hours	T_{ro}	h
Cost of material needed	C_m	€
Customer loss		
Time interval	Δt	yrs
Number of actual customer lost	C_a	
Number of potential customer lost	C_p	
Average revenue per customer	R_c	€/yr

Table 1: Factors associated with IT downtime costs (source: Dübendorfer et al. (2004))

[1] Currency depends on the actual user. Use Euro mark as an example.

2.4 Chapter conclusion

In this chapter, the basic concepts were described, in corresponding order of the research design. Start with the introduction of IS infrastructure and its interdependency. IS infrastructure was defined as *"a collection of technologies, people, and processes that facilitate large-scale connectivity and effective interoperation of an organization's IS application*" (Kumar, 2004, p. 11). There are four types of interdependencies exist with IS infrastructure. The basic interdependency within IS infrastructure was based on cyber connections. There was also physical interdependency when human beings joined in to provide inputs and collect output, which cannot be done by information system itself. IS infrastructure and company performance was based on logical interdependency that efficient improved by IS, in turn, the company invested more money to update IS to achieve higher performance.

According to literature, IS downtime was threatened by 9 factors: *natural disaster*, *hardware failure, software failure, and human error (inside or outside the company), system overload*, *computer virus/hacker attack, loss of network connectivity*, *power outage*, and *vandalism*. Those can result in *downtime loss, disaster recovery, liability,* and *customer loss. Downtime loss* can cause the direct financial losses. *A disaster recovery is* a special case only militates when the disaster occurs. The influences of *Liability* and *customer loss* do not directly occur as downtime happens.

Downtime includes three phases: *response phase, diagnostics phase*, and *repair phase.* Each phase has its related costs. Previous researchers mentioned seven downtime cost items: *Idle costs for equipment, idle costs for employees*, and *revenue losses, repair costs, liability costs, disaster recovery costs*, and *customer loss*. By putting the cost into the downtime reaction phases, we formulated the literature-based downtime costs model was: Total downtime Cost = idle costs of employees + idle costs of equipment + revenue losses +
repair costs + liability costs + disaster loss + customer loss

3 Methods

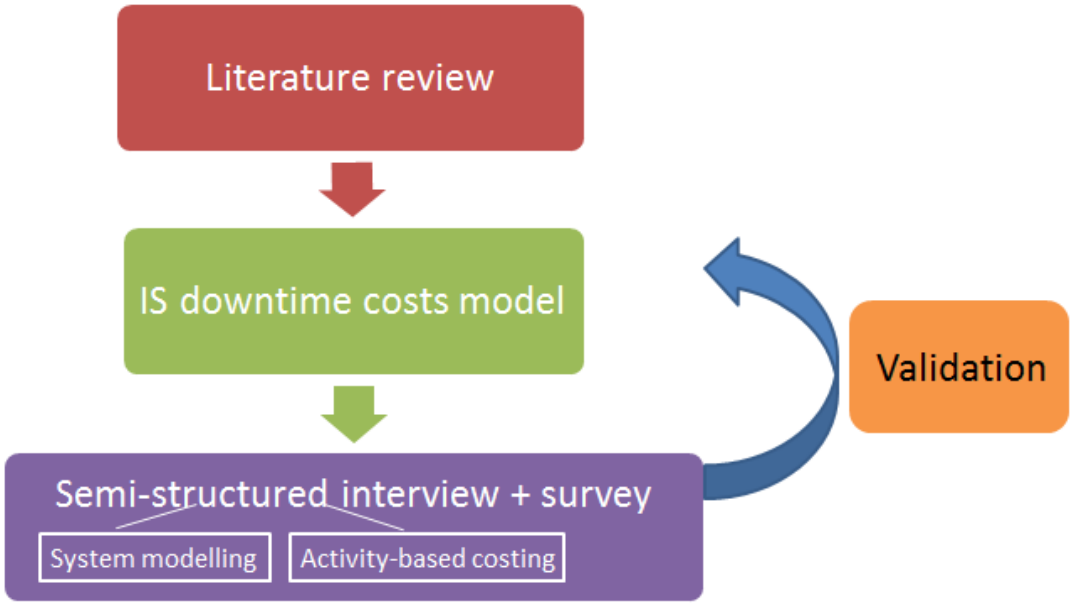

Figure 5: Research methods

In order to formulate a cost model to IS downtime to help companies to estimate their financial losses and to improve their IS infrastructure, the research starts with a systematic review of existing literature on IS downtime costs. Previous studies point out the focused downtime threats, different effects, and associated costs. However, the researchers did not provide enough practical evidence and the practicability of the model has not been tested.

Babbie (2010) stated that exploratory research was suitable for researchers who examine a new interest or the study of the top is relatively new. To achieve the main research question, conducting the exploratory research to explore the IS downtime causes and the effects in terms of processes and costs, makes the cost model generalizable to different kinds of companies. On the top of that, studying the existing literature to obtain a general understanding of the .Literature searching and analysing method described in section 3.1

The data collection method was discussed in section 3.2. In this thesis, the semi-structured interview is applied to get in-depth knowledge and test the theoretical model in the real world (3.3.1). According to Turner III (2010), the semi-structured interview is composed of extremely structured open-ended questions, where interviewees can express their knowledge and experience as much detailed as they desire. Besides, it also allows interviewers to ask follow-up questions. Due to the limited number of participants, surveys from recognised publishers were also taken into analysis.

Moreover, there are two tools are used in this research – system modelling and activity-based

costing to categorise the downtime effects and cost factors. System modelling allows for modelling the downtime affected components, processes, finding the interconnection of components, and categorising the downtime threats. The importance of modelling is that it provides a detailed map of the downtime damages for organizations. Activity-based costing offers information of costs based on each activity, which is helpful to identify the costs on a basis of business activities (3.2.2)

To detect the information from interviews and survey, we adopted the coding method developed by Creswell (2013) in section 3.3.

3.1 Searching and analysing literature

In order to present a wide-spread overview on the IS downtime costs in companies; a systematic search process was conducted. The following keywords were used for online research: information system infrastructure, information system interdependency, Causes of information system downtime/outage, information system downtime/outage costs, and information system maintenance.

Secondly, search the literature published in the academic database, such as Scopus and Web of Science as well as the search engine – Google Scholar from 2000 to 2016, where the searched keywords were included in the title, abstract, or keywords. Besides, in order to get a clear understanding of the term, some non-academic articles (e.g. white papers, reports from consulting agencies, and other online references) were included to enrich the searching results. A total of 96 articles were selected for further analysing. After that, all the articles were checked for removing duplicate articles. By reading the abstract of each article, the articles with pure technical scope were foreclosed from the list. Thereafter, 31 articles were deemed useful for this study. In analysing the articles, snowball method was applied to obtain other valuable references. In this research, reliability is based on selected databases, publications, the covered period and keywords which are documented for replication of the literature search process. The results of the reviewed articles were categorised based on the factors related to IS downtime costs (see Appendix A).

3.2 Data collection

In order to get the qualitative data, this study adopts semi-structured interviews due to the explorative nature of this thesis. Semi-structured interviews usually contain open-ended questions, which allows interviewees to fully express their viewpoints and experience (Turner III, 2010) and leaves room for the interviewee to improvise and ask follow up question (DiCicco-Bloom & Crabtree, 2006). Dealing with IS downtime can be treated as a dynamic process. Each company has its own unique IS infrastructure. This thesis aims to form a general applicable IS downtime costs model for different industries. Interviews can offer a deeper understanding of the empirical context of the study and check whether the assumptions and model discussed in the literature are aligned with practices.

3.1.1 Semi-structured interview

Participants

The interviewees are individuals from different industries whose company apply IS that they are using it in their daily work and have certain knowledge of the IS. In total, there were 10 participants joined the interview, of which 7 persons works for Chinese companies and 3 persons work for Dutch companies.

In social science studies, when the study group is highly selective and unrepresented of the entire population, it leads to an invalid research and conclusion cannot be drawn. The semi-structured interview has the potential to overcome the low rate of non-respondent and increase the number of question answered by respondents. Besides, it ensures validity by observing non-verbal indicators and answering the question without any assistance (Louise Barriball & While, 1994).

A primary concern in the interview is population validity. Due to time and costs constraints, in order to draw conclusions for the entire population; the sample obtained from the population must be representative of the same population.

Processes

To collect the qualitative data, interviews are conducted from 1st July to 30th September 2016. This includes minimum 30 to 60 minutes recorded interviews with the IS-related participants from different industries. The interview does not present any interviewee's name or their company name. The design of the interview questions follow the work of Moore, Dynes, and Chang (2015), where the questions are divided into three parts: grounding questions, macro-level questions and micro-level questions. This research adopts pilot studies to test the interview questions. The interview questions are listed in Appendix C.

3.1.2 System modelling and activity-based costing

When downtime occurs, it may affect some areas of business, determining the nature of downtime causes and the interdependencies of the initial trouble spot. It should be addressed that there are some unknown or unexpected consequences resulting from the downtime change that has influences on the others (Giaglis, 2001).

System modelling is contributing to guiding the building of components that related to downtime costs via analysis and simulation. Activity-based costing is considered as a more accurate way to calculating costs, through which managers can monitoring costs based on organizational resources assigned to each activity provides information on the costs of processes, products, activities and other costs. In this research, due to the lack of real cases, the activity-based costing used as a qualitative tool to categorise the underlying costs

3.2 Data analysis

In order to obtain accurate interview responses, this thesis follows the procedure developed by Creswell (2013). Starting with the *Organise and Prepare the Data for Analysis*, categorise the interview notes from different sources based on interview data, in an ascending order. Secondly, *Reading through All Data* provides an impression of the overall depth, credibility, and use of the information. Thirdly, *Coding the Data* categorise the terms addressed by participants into different groups. Fourthly, *Description/themes* generate a description of the setting or people and themes for analysis. Next, *Interrelating Themes/Description* narrows the responses to convey the findings of the analysis. Finally, *Interpreting the Meaning of Themes/Descriptions*, it allows using researcher's personal interpretation to state the findings confirm the previous information or diverge from it.

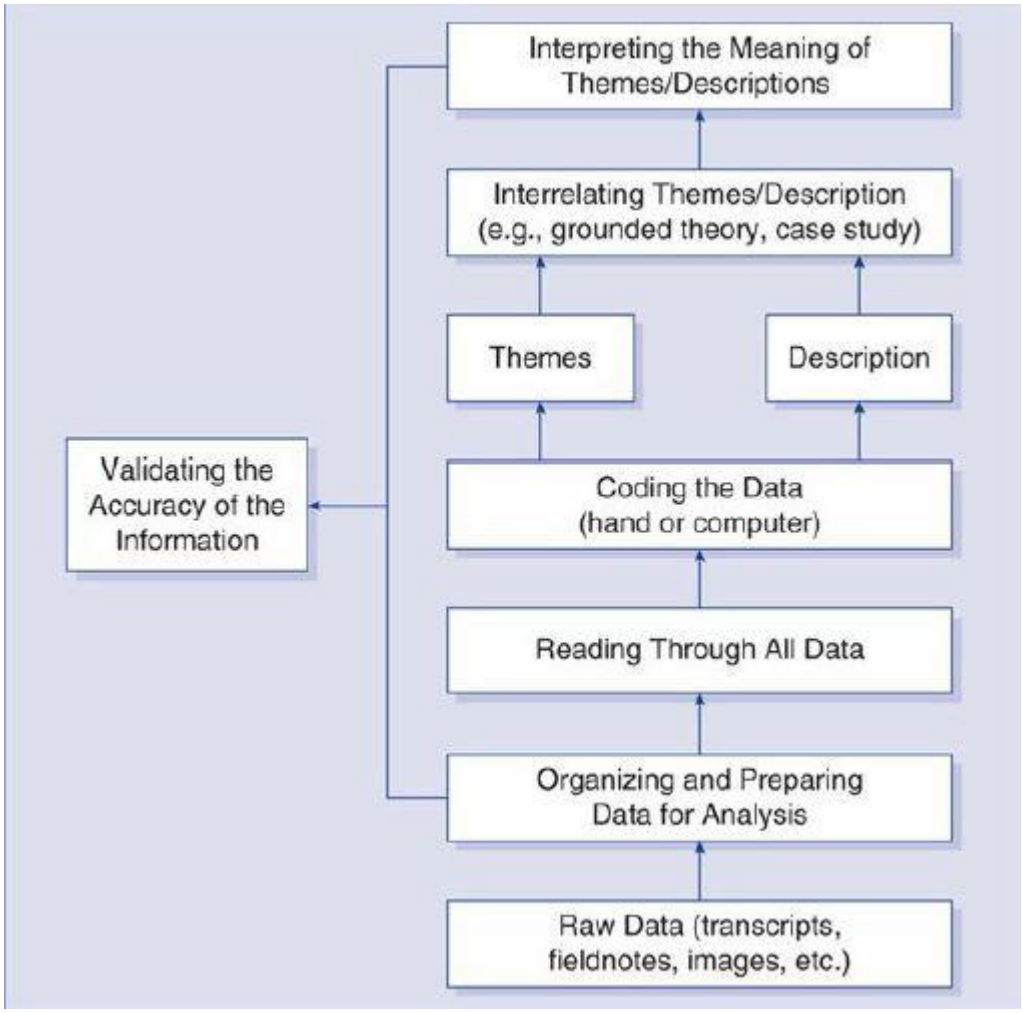

Figure 6: Data analysis process (source: Creswell (2013))

4 Analysis

In chapter 2.3.1, a linear costs model has already developed based on literature. This chapter elaborates the costs model from practical evidence. The semi-structured interviews provided insights into the problems, related consequences, and solving methods. There are 10 interviewees joined in this study, including 3 from the Netherlands and 7 from China. They are from transportation and storage, information and communication, financial and insurance activities, administrative and support service activities and education sector[2] with different positions and all have computer science background or work related to IT.

4.1 Company profiles

Every company has its uniqueness. We created a table containing the detailed information of all participants and their company, by categorising the companies into different industry following the ISIC codes, distinguishing the size of the company, and specifying the location of the company, which may determine the threats of downtime and can influence the downtime effects and losses (See Appendix D). Since our participants from two countries in two continents, we adopt ISIC codes, which is an international classification of industries.

4.2 Components and connects of phase sequence network during faults

According to the interviewees, there were two main findings need to be highlighted: firstly, IS downtime was a rare situation due to the application of autonomic computing systems. The high demands of IS infrastructure resulted in a sophistic network that people adopted software to handle the infrastructure. Therefore, researchers created the autonomic computing systems, which are self-configuration, self-optimizing, self-healing and self-protecting. With the help of the system, companies saved more time and money on managing the infrastructure (Jessup & Valacich, 2007). Secondly, companies had several backup systems and database. When the current one breaks down, the backup system or database starts automatically in a short period. The detailed interview results were established in the following sections

4.2.1 Sub-infrastructures and linkages

In section 2.1.1, sub-infrastructures of IS infrastructures had addressed, which had seven sub-infrastructures. In real life, these sub-infrastructures exists in companies, with slightly different components depends on the company type and size.

Interviewee 4 offers a new understanding of IS infrastructure that it includes two layers –basic operation system and upper business system. The operation system includes the monitoring of the internal memory, CPU, network flow, and so on. The business system refers to the

[2] The International Standard Industrial Classification (ISIC) is the industry standard classification system used in all nations. http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=27

standardisation of the system development – a special issuing system to ensure the correctness of code and manage the changes of code, the alert of unusual situation – special staff monitoring the system and fixing it when needed, and the and the multi-node systems – decreasing the system interdependency.

Hardware

The IS is built on the Server-Client network (Jessup & Valacich, 2007). There are several different kinds of server, while not ever company has its own server. Interviewee 1 mentioned that the downtime can be caused by the problems of an E-mail server. When the E-mail server breaks down, the whole E-mail system stops. Interviewee 4 and 5 talked about their web server. If the company highly relies on the internet, they build up their own web server for achieving high flexibility and reliability.

A notable finding from interviews was that desk computers were gradually replaced by smartphones, laptops, and other mobile devices. Desk computers used to be the basic element of IS system. Nowadays, these mobile devices offer people a more efficient and flexible working environment. While for managing essential data, corporate computers are needed and no personal things allowed linking to corporate IS network, for example, bank.

In order to protect data and ensure the constancy of business, big companies do not only have one IS and database. These companies have at least two systems and two different Data Centres located in different places to avoid geographic influences.

Software

In business, infrastructure monitoring tools (software) have been used for a long time, which help people to detect the unusual changes and inform these changes to technical staff. Interviewees reported that Enterprise Resource Planning (ERP) and Office Automation (OA) are widely adopted in the company for more efficient business management and information sharing. People put less effort than before in this monitoring process, therefore, it requires higher technical supports but less labour in this process.

Generally, the software is brought from specialised software providers. Most interviewees said that their company brought the business software from the software vendor, so there is no investment in software developing. Sometimes, the software providers may need to update or maintain the software; it requires the company to prepare for the changes, for instance, test the compatibility and reliability of the new version.

Communication and collaboration

E-mail is the widely used formal communication tool that applies for both internal and external communication. There is some other communication software, such as Skype, which are used for less formal communication. The Videoconference is used for long distance face-to-face communication, which requires high bandwidth.

In order to build a best-fit monitoring system, there are four rules need to follow: first of all, it can provide multiple alert methods, such as Short Message Service, email and so on; secondly, it should be customized; thirdly, it should support the operating system; finally, it needs to be capable with the desk help system (Hernantes, Gallardo, & Serrano, 2015)

Data and knowledge

Data has no meaning of itself. It can become meaningful by computing transmission and stores in the database. In this stage, data can be called information, which is useful to people or not. When the information is useful to someone, it becomes knowledge to the person.

Nearly all the interviewees mentioned the importance of Data Centre and some companies even have more than one Data Centre to protect data. Data offers the company to understand their customers, products, markets, and their business processes.

Facilities

It has to be noticed that not every company needs facilities such as, servers or power supply equipment. The main task of the facilities is to ensure the availability and security of IS infrastructure components (Jessup & Valacich, 2007).

As for the company that interviewee 1 and 6 worked, in order to ensure the continuity of IS, they have a backup system, which can launch automatically when the in-use system breaks down.

According to interviewee 9, as a teller, she needs to use the fingerprint scanner to log in a specific computer in order to start work.

Human resources

Every employee is a part of the IS infrastructure since they use the infrastructure. There are specialised IS staffs who build and maintain the IS system and employees who operate on it. When downtime happens, normal employees are the victim of the downtime. Their current tasks may be negatively affected by the breakdown. Technicians start to solve the problem.

Services

As for banks, IS system is developed internally and managed by internal experts in order to protect data. Other companies hire outside experts to build and manage the IS system but maintain a small part of the IS duties internally so as to reduce costs.

4.2.2 Connects of phase sequence network

By following the downtime causes addressed by literature, this part elaborates on how the downtime causes affect the IS infrastructure and business, by the means of comparing the literature with practical situation. Besides, due to the different geographic locations, there are some causes happened in China, while do not occur in the Netherlands. These differences are shown in Ishikawa diagram.

Downtime cause 1 – natural disasters

Natural disasters include a wide range of events, such as earthquake, tornado, severe thunderstorm, and so on. The impact of each event is various. Previous researches established a score card which evaluated the overall risk of certain event, in terms of likelihood, impact, and restoration time. For each factor, a scale from 0 to 10 was used to indicate the degree. Likelihood with 0 was not probable and 10 was highly probable. Impact with 0 was no impact and 10 was highly impact the existence of the company. The higher the number in Restoration time represented the longer restoration time ("Disaster Recovery: Best Practices," 2008).

Risk Assessment Form					
External risks					
Date:		Likelihood	Impact	Restoration Time	Score
Grouping	Risk	0 - 10	0 - 10	1 - 10	
Natural disasters					
	Earthquake	1	9	10	90
	Tornado	0	0	10	0
	Severe thunderstorm				0
	Hail	8	3	9	216
	Snow/ice/blizzard	9	5	8	360

Figure 7: Risk assessment form (source "Disaster Recovery: Best Practices" 2008))

As the image showed, snow/ice/blizzard was the most likely happened natural disaster, scored a 9, and also had a 5 and a 9 scored on impact and restoration time respectively. The overall score multiplied the three scores which got 360. It means that companies should pay more attention on preventing the possible losses that snow/ice/blizzard could make. However, there was no interviewee mentioned this cause.

Downtime cause 2 – hardware failure

The hardware, such as CPUs and Monitors, controls the network and the resources (Rosen, 1981). Once the hardware fails, it affects the business activities in a certain path.

Interviewee 1 talked about the failure of an E-mail server. As the name indicates, E-mail server handles the transaction of E-mails. If it gets trouble, the whole E-mail system cannot perform the work. Employees cannot use E-mail to communicate. While, there are some other alternative communication tools, such as Skype, QQ, and Video conference, which have the same function as E-mail. It has to be addressed that people in different countries may use different communication tools but the function of the tool is the same.

Interviewee 4, 7 and 8 stated that when the Data Centre or some essential parts of the IS system get damaged, the backup Data Centre or IS system starts automatically within a few minutes after the damage of the in-use one. As for small size companies, it is too expensive to build and maintain a backup system, therefore, they only have one system.

Downtime cause 3 – software failure

When specific requirements cannot be performed by the software, the company faces software problems (Callaghan & Mariappanadar, 2008). Interviewee 2 gave an example of the software failure – Microsoft SharePoint. A purchasing order was stopped in the approval process and the alarm did not work, which caused the supplier did not receive the order and none of us noticed the fault. One of the colleagues asked the factory if they received the goods, workers said no. We just found out that supplier did not receive our purchasing order." "We had to use air transport to deliver these goods. After that, they confirmed that the problem was due to the bug in the software itself.

Downtime cause 4– computer virus/hacker attack

The IS is under risks because some people seek for personal gratification by hacking computer networks or steal information from others. Although the security agencies put efforts on distancing computing resources from a variety of attacks and methods of data leaks, the computer hackers are constantly trying to find a more intuitive way for data access (Mehic et al., 2016).

Interviewee 7 mentioned that during the DDoS attack, there was no significant customer loss. Because the IS rebooted 4 hours later, 90% of services were back to normal one day after the attack, and 95% services could be offered 2 days later.

Interviewee 10 also gave an example of DDoS attack, which three attacks happened at the same time and had downtime for 30 minutes. During the downtime, he led to find out the attack source and solve the problem. The other employees were still working through their own devices, such as smartphones, to do tasks or contact customers, so there was no idle employee.

Downtime cause 5 – human error

Mindless and nonstandard operations incur human errors. The human error can occur during the change of IS management, in which the employees mistakenly transfer the code. As a result, the system may not perform the designed work or does not work at all, addressed by interviewee 8. Interviewee 10 offered another example that "the school needs to replace a certain IS component, while the person does not do enough prior tests and leads to the system breaks down."

Downtime cause 6 – vandalism

Vandalism refers to people deliberately damage the components or systems (Oz, 2009). Interviewee 5 gave an example. In his company, in order to protect data, the company set right management, in which everyone had their own authority to access files. The higher position you are, the more information you can access. If an employee tried to open the files that did not belong to his or her authority, the system blocked the employee ID or the device (company computer) atomically. This employee could not use the ID to log in on any devices until the IS colleagues unblocked the ID.

Downtime cause 7– system overload

In the case of system overload, the number of requests exceeds the capacity of the machine, which is not able to handle all the requests in a certain period (S. R. Ahuja & McHugh, 2013). Based on the interview results, the downtime caused by system overload is temporary, which can be solved in a short time. According to Interviewee 2 and interviewee 8, when there were too many people logged into a certain web page, the server could not process every request. Some people faced login failure that they had to try later.

Downtime cause 8 – loss of network connectivity

Interviewee 5 and 9 are the frontline service person, communicating with customers every day. This is a common downtime cause for both of them, while interviewee 5 experienced this kind of situation much more than interviewee 8, due to the different reliability of the system itself. Usually, it can be solved within 5 minutes. During that time, they handled the other demands of the customer. Therefore, interviewee 5 believed that this cause does not lead to any significant financial or customer losses since it is short and no idle employee or machine occurs.

Downtime cause 9 - Electronic power outage

Regarding the 10 interviews, there was only one person experienced a power outage 6 years ago and nearly all activities stopped for the company. None of the interviewees in the Netherlands had that experience.

The direct power outage in literature is the problem of power supply. Interviewee 1 worked in a small size company, where were 20 employees. They did not have extra power supply equipment and highly relied on the municipal power station. Without the power supply, the whole company cannot continue to work. Everyone had a day-off when the power outage occurred. However, some people might get phone calls from customers and they had to answer it. Some employees took their work home. When everyone went back to the office next day, the problem was solved. Therefore, the business went back on track. Besides, he added that if the company had another circuit, this situation could be avoided.

Downtime cause 10 – maintenance

Usually, the maintenance conducts during midnight that does not influence the company's activities. However, some maintenance actions have to be done during work times that lead to temporary downtime. For example, interviewee 10 mentioned misconfiguration, which happened before the system comes into service. In order to find the problem, it requires disabling certain software or hardware. The components rely on the disabled software or hardware cannot work as well.

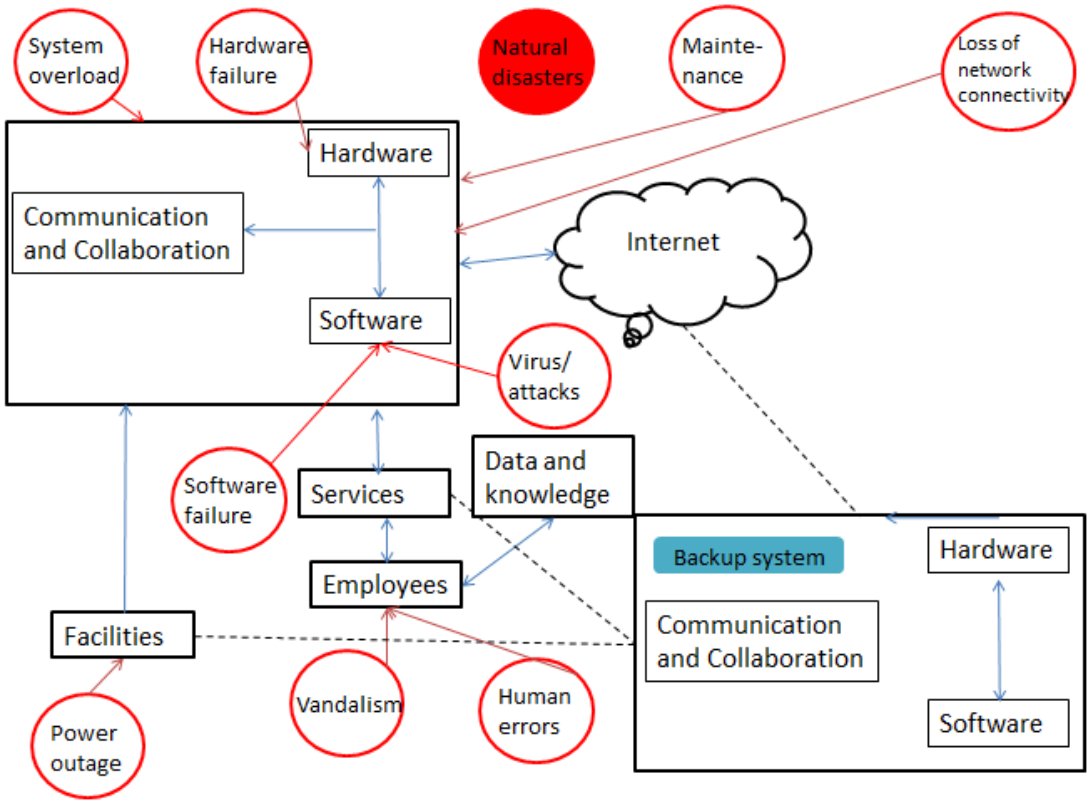

Figure 8: The downtime causes and impacts

The image below shows the detailed causes of downtime differences between literature and practices.

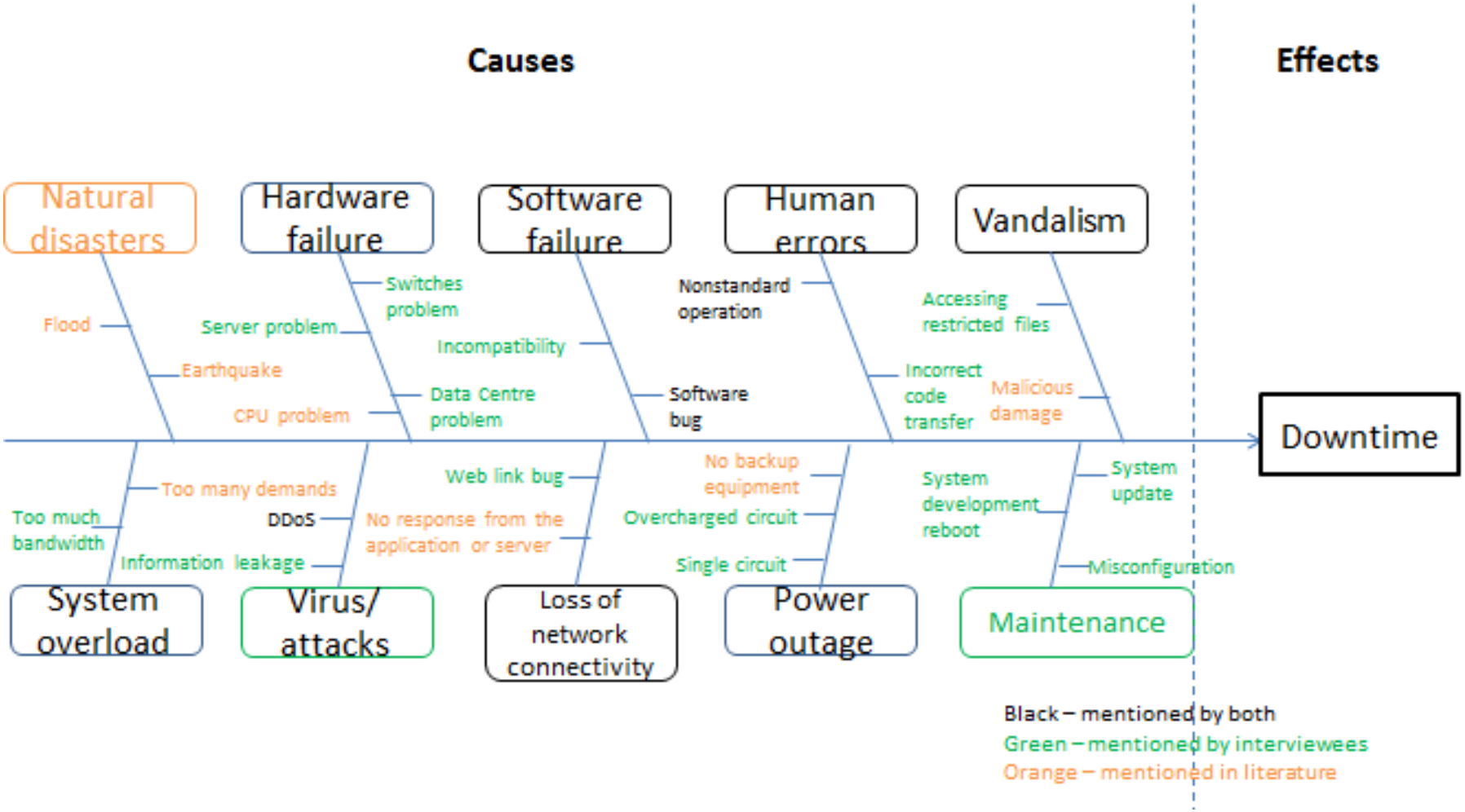

Figure 9: The different downtime causes between literature and interviews

4.3 Identifying the impacts and associated costs

4.3.1 Geographic differences

It can be noticed that the causes of downtime have significant differences between two countries. Problems related to electricity supply are only mentioned by participants from China, including power outage and circuit problem. Two interviewees – 8 and 10 mentioned DDoS attacks, while no interviewees from China gave downtime threats related to computer virus or attacks. Moreover, Dutch interviewees also mentioned human errors that Chinese interviewee did not talk about. Downtime threats mentioned by people from both countries were data centre damage, web link bugs, demands caused system overload and system update.

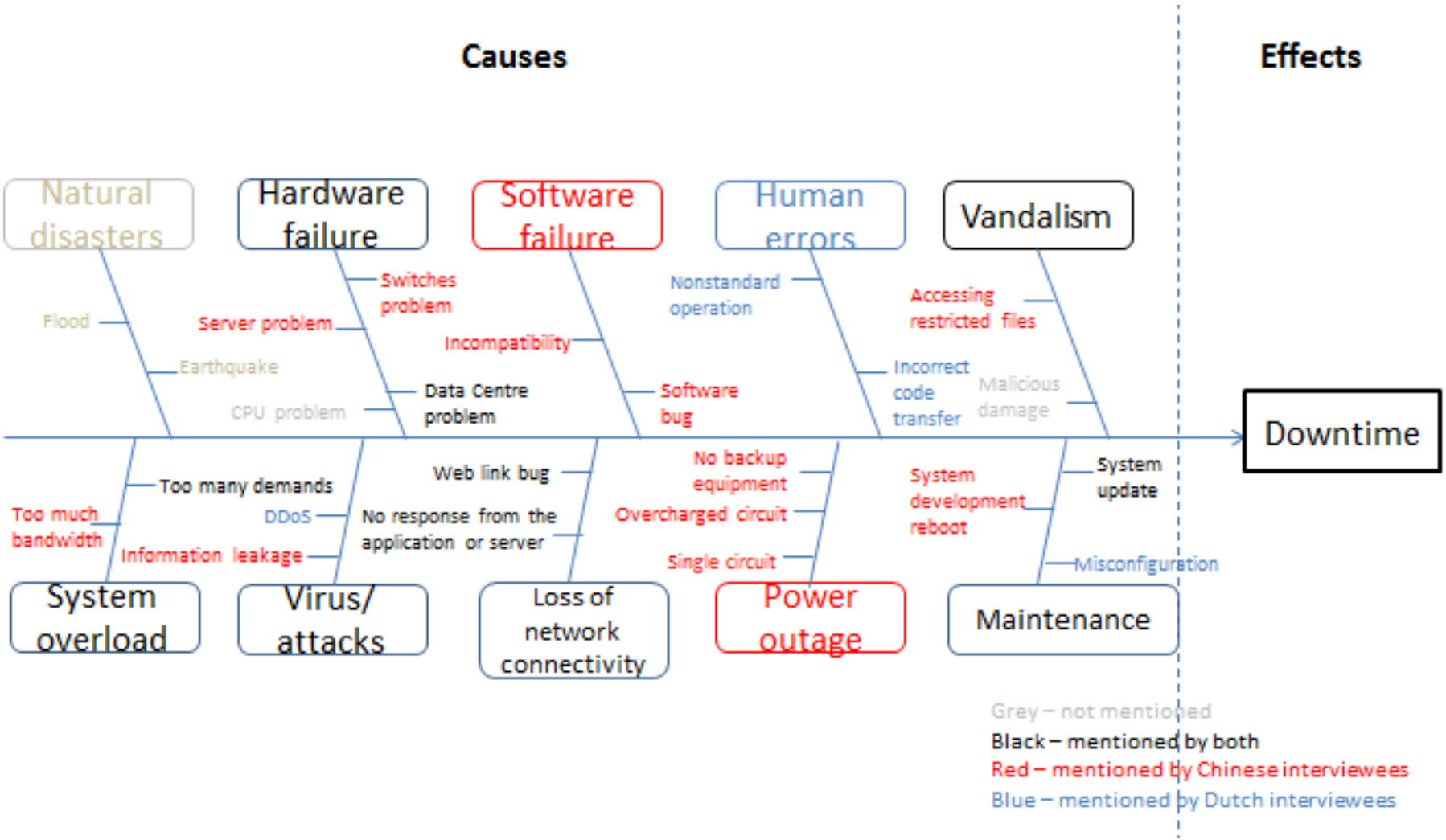

Figure 10: The different downtime causes between China and the Netherlands

4.3.2 Ranking the downtime threats

From the interview results, hardware failure was the most mentioned downtime threats. In the studies of Oz (2009), hardware failure was also the number one cause of downtime, due to the large number of computers, peripheral equipment, and communication media, which physical damages were more likely happened. The next most mentioned downtime causes from the interview were loss of network connectivity and system overload. The practical causes behind the loss of network connectivity were web link bugs and information leakage. Web link bugs can be caused by failures of the router, switches, hubs, and cables, which the client computers are not able to connect to certain web address ("Understanding Downtime," 2005). When companies face information leakage, cutting down the connection of network is the effective response to avoid further losses. The other second most mentioned cause was system overload. There were two main scenarios addressed by interviewees. If a machine received too many requests at the same time, it runs out of its capacity to handle the requests but still did not meet the request level. The machine was under risk of breakdown. Another one was the overcharge of bandwidth, resulting in the crash of server, and no network connection.

4.4 Chapter conclusion

In this chapter, we analysed the companies' IS infrastructures, which had the same sub-infrastructures with literature but the components were varied from companies, due to the different company's size and industry. The interviews added three downtime causes: system overload, loss of network connectivity, and maintenance. System overload is a man-made downtime that too many requirements were sent to a server which was over the capacity of the machine. Loss of network connectivity refers to access problem to web pages, which creates short time breakdowns. Maintenance is a planned downtime that the time and losses can be controlled by technicians. In addition, the causes of downtime has geographic differences between China and the Netherlands. China as a developing country, still suffers power outage. Interviewees from the Netherlands put emphasis on preventing computer virus/attacks and human errors.

5. Results

The downtime of IS does not only affect employees who use it, but also the business activities depend on it. In section 5.1, five effects of downtime in organisations are discussed. In the end, based on the effects and the associated costs, the cost model is shown.

5.1 Effects of downtime in organisations

Different types of downtime causes can generate the same consequence. In order to measure the costs of downtime, it is important to classify the effects. Five general effects were drawn from interviews.

5.1.1 Productivity declining

When IS breaks down, the information transfer time increases. In some companies, they use paper as an alternative mean to transfer information, which takes a longer time to share information.

5.1.2 Idle employees and equipment

Based on the responses from interviewees, the likelihood of idle employee and equipment is quite low nowadays but it still exists in the industry like the bank, where IS serves in national level. Once the downtime happens, it results in idle employees and equipment. Since the system is controlled by one host system, troubleshooting starts from the host system and narrows down. Therefore, it takes a longer time to detect problems in this kind of IS. The more organisations or layers IS serves, the longer MTTR is.

5.1.3 Liability

Downtime generates liability from two aspects. First of all, certain tasks do not complete due to the downtime, partners can ask for contractual penalties. Secondly, customers can also ask for compensations, if the company does not offer the agreed service level.

5.1.4 Damaged reputation

When the downtime occurs, the damaged degree of business activities depends on the breakdown point and its related components and employees. It might be difficult to evaluation the value of the company's reputation, while the value can reflect on the company's stock price, revenue and profitability ("Assessing the Financial Impact of Downtime: Understand the factors that contribute to the cost of downtime and accurately calculate its total cost in your organization," 2014). The reputation loss does not appear immediately after the

downtime but it can be affected by downtime in a long run.

5.1.5 Customer loss

When customers start to approaching competitors after downtime, the company suffers customer losses. According to interviewee 8, during the downtime caused by DDoS attack, there was no significant customer loss. Since the online banking still works for customers, they can do the transfer at home. In this sense, the degree of customer loss depends on the level of customers' satisfaction during downtime. The damage of customer loyalty is similar to which of reputation, exists for a long term, which mainly reflects on the revenue ("Assessing the Financial Impact of Downtime: Understand the factors that contribute to the cost of downtime and accurately calculate its total cost in your organization," 2014).

5.2 Costs of a downtime happening

This part aims to present the costs of downtime based on causes of downtime and correlated effects on organisations. Financial losses of downtime have two significant groups. The losses generate directly from the downtime victim, called direct costs. Another one is indirect costs which cannot be attributed to individual victims (Anderson et al., 2013).

5.2.1 Direct costs

Idle cost of employees

Since employees still receive their salary during the out-of-service state, it is important to know the amount of salary the idle employees received and the time they are idle. Next to that, collect the total normal working hours that employees work in a year, to get the amount of money that employees received per hour. And then, count the number of idle employees. The last factor is the idle time.

Idle cost of employees $= \frac{W_e}{T_e} \times T_i \times N_{ed} \times P_d$

Repair costs

This includes the material costs and external expert costs. To fix the downtime, the company may purchase new components to replace the old one or rent equipment, such as power supplement machine, to support the availability of business. In addition, when the internal employees are not able to repair the problem, the company may hire external experts to fix it, extra labour payments occurred.

Repair costs = $C_{bc} + C_e + C_r$

Compensation costs for work overtime

This is a special case that the problem cannot be solved within office hours that employees have to work outside the office hour. Therefore, the company has to pay extra money for work overtime. The overtime pay usually is higher than normal salary.

Compensation costs for work overtime = $N_b \times C_b \times T_b$

5.2.2 Indirect costs

Revenue loss

The financial losses of reputation damages, customer loss, and the productivity loss of equipment fall into this category. As addressed in section 4.3.3, the damages of reputation and customer do not immediately appear after the downtime, it may take some time reflecting on the revenue. In this case, it has to know the annual revenue, the time of operating, and the affected percentage from downtime.

Revenue loss = $\frac{\text{annual revenue}}{T_o} \times T_i \times \text{affected percentage}_d$

Compensation costs for customers and partners

When the downtime influence the service level, based on the service level agreements (SLAs), customers can ask for compensation. Besides, in a joint project, downtime occurred in one of the partners can impact on the entire project, so that the company needs to pay contractual penalties to the other partners.

Compensation costs for customers and partners = $CC_n \times CC_u + C_p + CC$

Total downtime costs = idle costs of employees + revenue loss + repair costs + compensation costs for work overtime + compensation costs for customers

Factor	**Symbol**	**Unit**
Idle cost of employees		
Employees' salary per year	W_e	€/yr[3]
Working time per employee per year	T_e	h/yr
Number of employees affected by downtime	N_{ed}	
Idle time	T_i	h
Repair costs		
Costs for replacing components	C_{bc}	€
Costs for hiring experts	C_e	€
Costs for renting equipment	C_r	€
Compensation costs for work overtime		
Number of employees in the team	N_b	
Overtime costs per hour for a	C_b	€/h

[3] Currency depends on the actual user. Use Euro mark as an example.

team member		
Work hours outside office hours	T_b	h
Revenue loss		
Total annual revenue	⊗	€/yr
Service operating hours per year	T_o	h
Part of the revenue affected by downtime	$⊗_d$	
Compensation costs for customers and partners		
Number of claimants	CC_n	
Unit spending of required compensation	CC_u	€
Claims from contractual penalties	C_p	€
Other related costs	CC	€

Table 2: Revised factors associated with IT downtime costs

5.3 Chapter conclusion

This chapter presented the new downtime costs model, by categorising downtime effect and corresponding costs. We find five downtime damages: idle employees and equipment, productivity losses, liability, reputation damages, and customer losses. Besides, there are five cost categories: idle costs of employees, repair costs, compensations for work over time, revenue losses, and compensations for customers and partners. The first three are direct losses when downtime occurs. And the other two do not directly generate as cash outlay. Idle employees and equipment generate a direct loss for idle employees since the company still paid for employees during the downtime. Another two direct costs are: repair costs and compensation costs for work overtime. These occur during the repair phases. Two indirect costs are revenue losses and compensation costs for customers and partners. In this research, revenue losses come from productivity losses, damaged reputation, and customer losses. During downtime, the company may not perform the agreed performance that generated negative influence on reputation and customers. This leads to potential liability, which customers and partners may ask for compensations regarding contact.

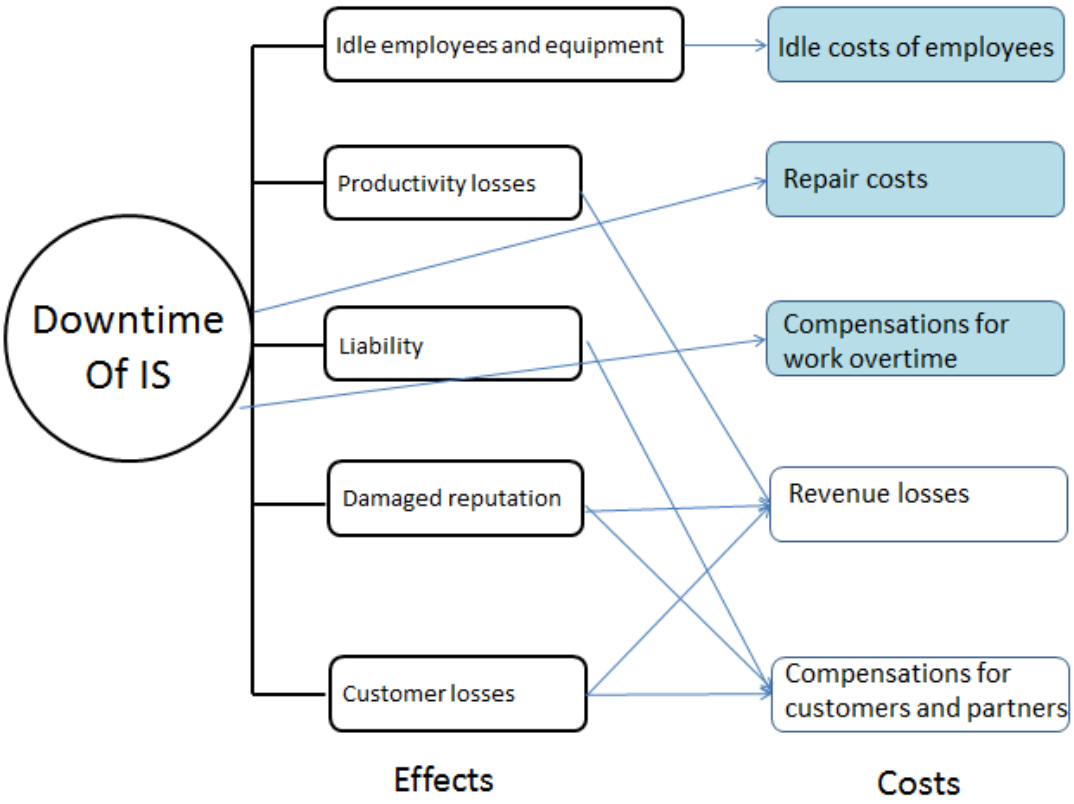

Figure 11: IS downtime effects and related costs

6. Validation

According to the Handbook for the Quality Assurance of Metrological Measurements, "method validation consists of documenting the quality of an analytical procedure, by establishing adequate requirements for performance criteria, such as accuracy, precision, detection limit, etc. and by measuring the values of these criteria" (Taylor & Opperman, 1986).

The purpose of this section is to validate the interview-based model through comparing the performance parameters of the literature-based model with which developed during interviews. Secondly, 3 surveys were included in this section to evaluate whether the interview-based model fits for a wide range of applications.

6.1 Changes of the new costs model

Modelling the new costs model follows two rules. Firstly, omit the duplicated cost items. Secondly, add new cost items based on interviews and reality.

6.1.1 Duplicated cost factors

In the literature-based model, disaster loss was put as an individual category. The natural disaster is a special case but related costs are not. During the disaster recovery period, the company still pays salary to employees. Some employees join the recovery team, while the other cannot do anything. These people become idle labour, which can be calculated by *idle cost of employees*. Besides, the *cost of necessary material* is the same as *costs for replacing components* and *costs for renting equipment*, belonged to *repair costs*. *Recovery work hours beyond office hours* is assigned to a new category called *Compensation costs for work overtime*. Another duplicated cost is *idle costs of equipment*. The idle equipment negatively influences the overall productivity. It is unable to produce expected goods during downtime. Therefore, it results in the loss of revenue. In some cases, the company has a joint project with other companies and the downtime can delay the whole process of the project. Based on the contract, the company which suffers downtime needs to take responsibility for the delay. Downtime can also incur the under-service compensation for customers. Thus, in the new model *compensation costs for customers and partners is added.*

6.1.2 New cost factors

In order to make the business run at normal state, the company may ask the technicians work outside the office hour, therefore, continue *compensation costs for work overtime* is generated.

6.2 Downtime costs in real cases

Although the unplanned downtime accounts for 10% of all downtime, damages of unplanned downtime much exceed which of planned downtime, due to its unexpected nature ("Assessing the Financial Impact of Downtime: Understand the factors that contribute to the cost of downtime and accurately calculate its total cost in your organization," 2014). A notable unplanned downtime was Data Centre outages, revenue loss was placed in the second position, which resulted in $13,141,737 losses (*Cost of Data Center Outages*, 2016). Survey results from SearchCIO showed that IS downtime was still a threat to companies, which 75% companies suffered downtime ("Trends in high availability and fault tolerance," 2010).

As for companies in the Netherlands, since the power outage is rare, there are no strategies or emergency actions for power outage based on interviews. The recent large power outage was on 27th March, 2015. News reported by Escritt (2015) showed that a power outage hit northern Holland, including Amsterdam and Schiphol Airport. People were trapped in trams and metros, because the doors opened electronically. Besides, it also caused server delay of trains and airplanes, since it was controlled and monitored by IT system. The power supply was gradually back to normal two hours after the start of outage. The outage was caused by two factors: one was the failure of components drive, the other one was a follow-up employee error, which made incorrect interpretation (Pieters, 2015). During the two hours, due to the lack of power supplement equipment, neither governments nor companies could get electricity immediately. However, according to the interview answers and news from China, the power outage caused downtime is one of the underlying threats to IT infrastructure continuity. One Chinese interviewee reported an unplanned power outage downtime in 2006, which made most of the company's activities were stopped. As a matter of fact, power outage is a planned downtime in China nowadays ("国网哈尔滨供电公司关于部分线路停电的通知," 2016; "秦皇岛停电通知," 2016). In order to keep the business running, most of the companies prepare extra power supply equipment for offering electricity. In this sense, even the unplanned power outage occurs, the companies can still run as normal.

7. Conclusion

Understanding IS infrastructure becomes complex due to the large demand of information demands. This also challenges the company's ability to solve IS related problems. Therefore, we studied the interdependency of IS infrastructure, causes of IS downtime, related effects, and corresponding costs. On the other hand, the result of this study may also help to prevent the organization from huge financial losses.

Sub-question 1: how is the IS infrastructure related to its environment?

This research find out two types of interdependencies addressed by Rinaldi et al. (2001): cyber and logical interdependency. Basically, in a company, the foundation of IS infrastructure is the cyber connections, where information transfers mutually from one device to another. Logical interdependency exists between the interactions of human beings and the cyber system. Employees use their knowledge to manage the IS via services. In turn, the valuable data and knowledge store as intellectual property to offer insights of IS.

Sub-question 2: what are the causes of IS downtime?

There are 10 main causes that threat the health of IS, which are *natural disaster*, *hardware failure*, *software failure*, *and human error*, *system overload*, *computer virus/hacker attack*, and, *loss of network connectivity*, *power outage*, *vandalism*, and *maintenance*. The natural disaster is the extreme situation, which do not mention by interviewees or surveys. However, it cannot be ignored by managers. Natural disaster does happen in other companies and countries. Hardware and software failures are the most mentioned downtime causes. However, there is a significant difference of IS downtime cause between China and the Netherlands. Due to the different sovereign state between China and the Netherlands, power outage is still the main threat of IS in China, while, it is rare in the Netherlands.

Sub-question 3: what are the effects of IS downtime?

When downtime happened, the system cannot perform the agreed work. It incurs the corresponding damages, such as *idle employees and equipment*, *productivity losses*, *liability*, *reputation damages*, and *customer losses*.

Sub-question 4: what are the costs of these IS downtime effects?

Based on the damages of IS downtime, there comprise of two types of downtime costs: direct and indirect costs. Direct costs refer to the losses generate directly from the downtime victim. Indirect costs cannot be attributed to individual victims (Anderson et al., 2013). There is one direct link between the *costs of idle employee* and *idle employee and equipment*. Two direct expenses related to the fix of the system are *repair costs* and *compensations for work overtime*. Indirect costs generated from *productivity declining, liability, damaged reputation*, and *customer loss*, are *revenue loss* and *compensations for customers and partners*.

Main research question: How to calculate the downtime costs of IS infrastructure?

To calculate the downtime costs of IS infrastructure, companies should have a clear

understanding of their IS infrastructure and how the components link with each other. Next, detecting and identifying the causes of downtime is important. Based on the causes, managers can know what kind of damages the downtime incurs for the company's financial performance. Regarding the damages, we developed the corresponding financial losses and formulate the equation as follows:

Total downtime costs = idle costs of employees + revenue loss + repair costs + compensation costs for work overtime + compensation costs for customers

The new cost model distinguishes between two types of costs. The direct costs generate from specific targets, including idle costs of employees, repair costs, and compensation costs for work overtime. The indirect costs refer to the long-term costs that are not directly affected by the downtime, including revenue losses and compensation costs for customers. In this way, by linking the downtime effects with the cost factors, it avoids the duplicated cost factor and finds out new underlying items. Besides, the literature-based cost model had several shortcomings: first of all, it contained repeated cost items. In the case of disaster, the company has to rebuild or repair its facilities, which is the same as repair costs. Therefore, disaster cost is a special cost of repair cost. Secondly, the old model did not distinguish between direct and indirect costs, which resulted in missing factors.

When organizations understand the causes of downtime and related costs, companies can better manage their IS infrastructure in order to preventive downtime. The company's downtime losses are significantly lower than which does not prepare.

8. Limitations and future studies

The limitations of this research are as follows: first of all, due to the time constraints, there were 10 participants joined the interview. Secondly, the interviewer's presence may bias responses (Creswell, 2013). The interviewees can be influenced by interviewer's behaviour, although I try to not show any interferential behaviour during interviews. Thirdly, the nature of the study is qualitative research, so the accurate results of financial losses do not include in this research.

In the future studies, researchers can investigate in the way that companies do to keep the IT system away from downtime. Besides, to make the cost model more accurate, researchers can apply the proposed model in an organization, collecting more details of downtime effect and the cost factors. A case study would be suitable in this case. Another research direction can be to what extent does the company benefits from the downtime preventive program. Although preparing for the possible downtime can significantly reduce the losses, the money invests in the prevention program can be huge.

Acknowledgement

I hereby like to express my gratitude to my supervisors, Prof. Dr. Nieuwenhuis and Mr. Abhishta for their engagement and supports in my research. All the feedbacks and the smooth communication have made a significant contribution to the quality of this thesis.

My gratitude also goes out to all the interviewees, who shared their precious time and valuable insights. They provided me with a lot of practical evidence, which enriches the content of this thesis.

Last but not least, I would like to state my appreciation to my family and friends, who support and listen to me during the difficult times as well as keep me motivated during the whole graduation processes. Therefore, I have the thesis as it today.

References

Ahuja, I. P. S., & Khamba, J. S. (2008). Total productive maintenance: literature review and directions. *International Journal of Quality & Reliability Management, 25*(7), 709-756.

Ahuja, S. R., & McHugh, J. G. (2013). System and method for avoiding system overload by maintaining an ideal request rate: Google Patents.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., . . . Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265-300). Berlin, Heidelberg: Springer Berlin Heidelberg.

Assessing the Financial Impact of Downtime: Understand the factors that contribute to the cost of downtime and accurately calculate its total cost in your organization. (2014). Retrieved from http://www.visionsolutions.com/docs/default-source/white-papers/wp_financialimpact_e.pdf?sfvrsn=4

Babbie, E. (2010). Research Design *The Practice of Social Research* (pp. 92). The United States: Wadsworth, Cengage Learning.

Becker, M., Goldszal, A., Detal, J., Gronlund-Jacob, J., & Epstein, R. (2015). Managing a Multisite Academic–Private Radiology Practice Reading Environment: Impact of IT Downtimes on Enterprise Efficiency. *Journal of the American College of Radiology, 12*(6), 630-637. doi:http://dx.doi.org/10.1016/j.jacr.2014.11.002

Bharadwaj, A. S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly, 24*(1), 169-196. doi:10.2307/3250983

Bhatt, G. D., & Grover, V. (2005). Types of Information Technology Capabilities and Their Role in Competitive Advantage: An Empirical Study. *Journal of Management Information Systems, 22*(2), 253-277.

Bosse, S., Splieth, M., & Turowski, K. (2016). Multi-objective optimization of IT service availability and costs. *Reliability Engineering & System Safety, 147*, 142-155. doi:http://dx.doi.org/10.1016/j.ress.2015.11.004

Bowen, J. (2013). *Towards Verified Systems*: Elsevier Science.

Broadbent, M., Weill, P., Clair, D. S., & Kearney, A. T. (1999). THE IMPLICATIONS OF INFORMATION TECHNOLOGY INFRASTRUCTURE FOR BUSINESS PROCESS REDESIGN. *MIS Quarterly, 23*(2), 159-182.

Byrd, T. A., & Turner, D. E. (2000). Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct. *Journal of Management Information Systems, 17*(1), 167-208.

Caccamo, M., Buttazzo, G., & Lui, S. (2000, 2000). *Capacity sharing for overrun control.* Paper presented at the Real-Time Systems Symposium, 2000. Proceedings. The 21st IEEE.

Callaghan, K. O., & Mariappanadar, S. (2008). Restoring service after an unplanned IT

outage. *IT Professional, 10*(3), 40-45.

Campbell, E. M., Sittig, D. F., Guappone, K. P., Dykstra, R. H., & Ash, J. S. (2007). *Overdependence on technology: an unintended adverse consequence of computerized provider order entry.* Paper presented at the AMIA.

Chang, Q., Ni, J., Bandyopadhyay, P., Biller, S., & Xiao, G. (2007). Maintenance staffing management. *Journal of Intelligent Manufacturing, 18*(3), 351-360. doi:10.1007/s10845-007-0027-7

Chanopas, A., Krairit, D., & Khang, D. B. (2006). Managing information technology infrastructure: a new flexibility framework. *Management Research News, 29*(10), 632-651. doi:doi:10.1108/01409170610712335

Cost of Data Center Outages. (2016). Retrieved from http://www.emersonnetworkpower.com/en-US/Resources/Market/Data-Center/Latest-Thinking/Ponemon/Documents/2016-Cost-of-Data-Center-Outages-FINAL-2.pdf

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications.

Cronholm, M. (2000). *Thermography's impact on economic performance: minimizing the cost of downtime and maintenance*.

Dübendorfer, T., Wagner, A., & Plattner, B. (2004). *An economic damage model for large-scale internet attacks.* Paper presented at the Enabling Technologies: Infrastructure for Collaborative Enterprises, 2004. WET ICE 2004. 13th IEEE International Workshops on.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education, 40*(4), 314-321. doi:10.1111/j.1365-2929.2006.02418.x

Disaster Recovery: Best Practices. (2008). Retrieved from http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-453495.pdf

Duncan, N. B. (1995). Capturing Flexibility of Information Technology Infrastructure: A Study of Resource Characteristics and their Measure. *Journal of Management Information Systems, 12*(2), 37-57.

Escritt, T. (2015). Power returns to Amsterdam after outage hits a million homes. Retrieved from http://www.reuters.com/article/us-dutch-power-outages-idUSKBN0MN0UJ20150327

Franke, U. (2012). Optimal IT service availability: Shorter outages, or fewer? *Network and Service Management, IEEE Transactions on, 9*(1), 22-33.

Franke, U., Johnson, P., & König, J. (2014). An architecture framework for enterprise IT service availability analysis. *Software & Systems Modeling, 13*(4), 1417-1445. doi:10.1007/s10270-012-0307-3

Friedman, J. H. (1998). Data Mining and Statistics: What's the connection? *Computing Science and Statistics, 29*(1), 3-9.

Gable, G. G., Sedera, D., & Chan, T. (2008). Re-conceptualizing information system success: The IS-impact measurement model. *Journal of the association for information systems, 9*(7), 377.

Giaglis, G. M. (2001). A Taxonomy of Business Process Modeling and Information Systems Modeling Techniques. *International Journal of Flexible Manufacturing Systems,*

13(2), 209-228. doi:10.1023/a:1011139719773

Halligan, D. W., Demsetz, L. A., Brown, J. D., & Pace, C. B. (1994). Action‐Response Model and Loss of Productivity in Construction. *Journal of Construction Engineering and Management, 120*(1), 47-64. doi:doi:10.1061/(ASCE)0733-9364(1994)120:1(47)

Harris, C. (2011). IT Downtime Costs $26.5 Billion In Lost Revenue. Retrieved from http://www.informationweek.com/it-downtime-costs-$265-billion-in-lost-revenue/d/d-id/1097919

Hernantes, J., Gallardo, G., & Serrano, N. (2015). IT Infrastructure-Monitoring Tools. *IEEE Software, 32*(4).

Hughes, J., & James, K. (2009). Where IT infrastructure and business strategy meet. Retrieved from http://www.mckinsey.com/business-functions/business-technology/our-insights/where-it-infrastructure-and-business-strategy-meet

Jessup, L., & Valacich, J. (2007). Managing the information systems infrastructure *Information Systems Today: Managing the Digital World*: Prentice Hall.

Kumar, R. L. (2004). A framework for assessing the business value of information technology infrastructures. *Journal of Management Information Systems, 21*(2), 11-32.

Labib, A. W. (1998). World‐class maintenance using a computerised maintenance management system. *Journal of Quality in Maintenance Engineering, 4*(1), 66-75. doi:doi:10.1108/13552519810207470

Lei, J., Guan, P., Gao, K., Lu, X., Chen, Y., Li, Y., . . . Zheng, K. (2014). Characteristics of health IT outage and suggested risk management strategies: An analysis of historical incident reports in China. *International Journal of Medical Informatics, 83*(2), 122-130. doi:http://dx.doi.org/10.1016/j.ijmedinf.2013.10.006

Louise Barriball, K., & While, A. (1994). Collecting Data using a semi‐structured interview: a discussion paper. *Journal of advanced nursing, 19*(2), 328-335.

Low, H. (2015). How to improve system availability and minimize down time with Hercules™ MCUs? *Texas Instrument*.

Mehic, M., Slachta, J., & Voznak, M. (2016). Whispering through DDoS attack. *Perspectives in Science, 7*, 95-100. doi:http://dx.doi.org/10.1016/j.pisc.2015.11.016

Mercer, C. W., Savage, S., & Tokuda, H. (1994, 15-19 May 1994). *Processor capacity reserves: operating system support for multimedia applications*. Paper presented at the Multimedia Computing and Systems, 1994., Proceedings of the International Conference on.

Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cybersecurity investment. *Available: Southern Methodist University. Available at: http://blog. smu. edu/research/files/2015/10/SMU-IBM. pdf (Accessed 2015-12-14)*, 32.

Oz, E. (2009). Risks, Security, and Disaster Recovery *Management Information Systems* (pp. 476): Thomson.

Pascual, R., Meruane, V., & Rey, P. (2008). On the effect of downtime costs and budget constraint on preventive and replacement policies. *Reliability Engineering & System Safety, 93*(1), 144-151.

Patterson, D. A. (2002). *A Simple Way to Estimate the Cost of Downtime.* Paper presented at the LISA.

Pieters, J. (2015). EMPLOYEE ERROR CAUSED POWER OUTAGE AT SCHIPHOL, N. NETHERLANDS. Retrieved from http://www.nltimes.nl/2015/06/12/employee-error-caused-power-outage-at-schiphol-n-netherlands/

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage: Harvard Business Review, Reprint Service.

Prasad Nepal, M., & Park, M. (2004). Downtime model development for construction equipment management. *Engineering, Construction and Architectural Management, 11*(3), 199-210.

Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). *Cyber-physical systems: the next computing revolution*. Paper presented at the Proceedings of the 47th Design Automation Conference, Anaheim, California.

Ramirez, R., Melville, N., & Lawler, E. (2010). Information technology infrastructure, organizational process redesign, and business value: An empirical analysis. *Decision Support Systems, 49*(4), 417-429. doi:http://dx.doi.org/10.1016/j.dss.2010.05.003

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems, 21*(6), 11-25. doi:10.1109/37.969131

Rosen, E. C. (1981). Vulnerabilities of network control protocols: an example. *SIGCOMM Comput. Commun. Rev., 11*(3), 10-16. doi:10.1145/1015591.1015592

Saaksjarvi, M. (2000). The Roles of Corporate IT Infastructure and their Impact on IS Effectiveness. *ECIS 2000 Proceedings*, 90.

Saied, A., Overill, R. E., & Radzik, T. (2016). Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing, 172*, 385-393. doi:http://dx.doi.org/10.1016/j.neucom.2015.04.101

Sieklik, B., Macfarlane, R., & Buchanan, W. J. (2016). Evaluation of TFTP DDoS amplification attack. *Computers & Security, 57*, 67-92. doi:http://dx.doi.org/10.1016/j.cose.2015.09.006

Takezawa, N., Nakahara, K., Uenohara, Y., Takayama, M., & Okuda, H. (2010). Reliability evaluation system, reliability evaluating method, and reliability evaluation program for information system.

Taylor, J. K., & Opperman, H. V. (1986). Handbook for the quality assurance of meteorological measurements. Gaithersburg, Md: National Bureau of Standards.

Trends in high availability and fault tolerance. (2010). Retrieved from http://searchcio.techtarget.com/podcast/Trends-in-high-availability-and-fault-tolerance

Tsimberdonis, A. I., & E. Lile Murphree, J. (1994). Equipment Management through Operational Failure Costs. *Journal of Construction Engineering and Management, 120*(3), 522-535. doi:doi:10.1061/(ASCE)0733-9364(1994)120:3(522)

Turner III, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. *The qualitative report, 15*(3), 754.

Understanding Downtime. (2005). Retrieved from https://technet.microsoft.com/en-us/library/aa998704(v=exchg.65).aspx

Valacich, J., & Schneider, C. (2010). Managing the Information Systems Infrastructure

Information Systmes Today: Managing the Digital World: Pearson.

Zambon, E., Etalle, S., Wieringa, R. J., & Hartel, P. (2011). Model-based qualitative risk assessment for availability of IT infrastructures. *Software & Systems Modeling, 10*(4), 553-580. doi:10.1007/s10270-010-0166-8

Zardini, A., Rossignoli, C., & Ricciardi, F. (2016). A bottom-up path for IT management success: From infrastructure quality to competitive excellence. *Journal of Business Research, 69*(5), 1747-1752. doi:http://dx.doi.org/10.1016/j.jbusres.2015.10.049

国网哈尔滨供电公司关于部分线路停电的通知. (2016). Retrieved from http://www.harbin.gov.cn/info/news/index/detail/439921.htm

秦皇岛停电通知. (2016). Retrieved from http://www.tstdtz.com/tags/%E7%A7%A6%E7%9A%87%E5%B2%9B%E5%81%9C%E7%94%B5%E9%80%9A%E7%9F%A5

Appendix

Appendix A: Keywords used for searching in Scopus, Web of Science and Google Scholar

Keywords	Title	Authors	Publish year
Information system infrastructure and interdependency	A bottom-up path for IT management success: From infrastructure quality to competitive excellence	Zardini, Rossignoli, and Ricciard	2016
	Managing a Multisite Academic–Private Radiology Practice Reading Environment: Impact of IT Downtimes on Enterprise Efficiency	Becker et al.,	2015
	Information technology infrastructure, organizational process redesign, and business value: An empirical analysis	Ramirez, Melville, and Lawler	2010
	Managing the Information Systems Infrastructure	Valacich and Schneider	2010
	Where IT infrastructure and business strategy meet	Hughes and Kaplan	2009
	Managing the information systems infrastructure	Jessup and Valacich	2007
	Managing information technology infrastructure: a new flexibility framework	Chanopas, Krairit, and Khang	2006
	Types of Information Technology Capabilities and Their Role in Competitive Advantage: An Empirical Study	Bhatt and Grover	2005
	A framework for assessing the business value of information technology infrastructures	Kumar	2004
	Identifying, understanding, and analyzing critical infrastructure interdependencies	Rinaldi, Peerenboom, and Kelly	2001
	A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation	Bharadwaj	2000
	Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct	Byrd and Turner	2000

	The Roles of Corporate IT Infastructure and their Impact on IS Effectiveness	Saaksjarvi	2000
	The Implications of Information Technology Infrastructure for Business Process Redesign	Broadbent, Weill, Clair, and Kearney	1999
	Capturing Flexibility of Information Technology Infrastructure: A Study of Resource Characteristics and their Measure	Duncan	1995
Causes and effects of IS downtime	Aircraft Scheduled Airframe Maintenance and Downtime Integrated Cost Model	Salto et al.	2016
	Multi-objective optimization of IT service availability and costs	Bosse et al.	2016
	Characteristics of health IT outage and suggested risk management strategies: An analysis of historical incident reports in China.	Lei et al.	2014
	An architecture framework for enterprise IT service availability analysis	Franke et al.	2014
	Optimal IT service availability: Shorter outages, or fewer?	Franke	2012
	Restoring service after an unplanned IT outage	Callaghan and Mariappanadar	2008
	On the effect of downtime costs and budget constraint on preventive and replacement policies	Pascual, Meruane, and Rey	2008
	Re-conceptualizing information system success: The IS-impact measurement model	Gable et al.	2008
	Processor capacity reserves: operating system support for multimedia applications	Mercer, Savage, and Tokuda	1994
Reactions to downtime	Total productive maintenance: literature review and directions	I. P. S. Ahuja and Khamba	2008
	Maintenance staffing management	Chang et al.	2007
	Downtime model development for construction equipment management	Prasad Nepal and Park	2004
	World - class maintenance using a computerised maintenance management system	Labib (1998)	1998
Costs of downtime	An economic damage model for large-scale internet attacks	Dübendorfer, Wagner, and Plattner	2004
	Thermography's impact on economic performance: minimizing the cost of downtime and maintenance	Cronholm	2000

	Equipment Management through Operational Failure Costs	Tsimberdonis and Murphree	1994

Appendix B: interview framework

First of all, thank you for you participation of this interview. This interview will be in the following parts:

- Company profile
- Respondent profile
- Knowledge on IT downtime
- Reactions to IT downtime
- Knowledge on downtime minimisation and avoidance

1. Company profile

This part of interview will record the information of your company on the basis of ISIC[4] codes. The name of your firm or any other information will keep anonymously.

2. Respondent profile

In order to provide an unbiased study, questions will aim at knowing participants' experience and work area. Besides, questions on the importance of IT infrastructure will also be asked to know participants' overall understanding of their IT infrastructure.

3. Knowledge on IT downtime

This part aims at understanding the downtime threats faced by your organization and the way these threats affected your organization. I would also like to know the frequency of the downtime and costs if participants can offer.

4. Reactions to IT downtime

This parts aims at knowing the procedures and actions done after downtime happening.

5. Knowledge on downtime minimisation and avoidance

In this part, I would like to know if some kinds of downtime can be eliminated. Therefore, the costs of related causes of downtime can also be avoided.

[4] The International Standard Industrial Classification (ISIC) is the industry standard classification system used in all nations.
http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=27

Appendix C: Interview questions

Thank you for your participation in this interview. My name is Qin Li from University of Twente. I am currently doing my master thesis about modelling the costs of IT downtime. Based on literature review, some basic and general information is obtained, while,
The purpose of doing this interview is to get more insights in IT infrastructure and IT downtime, in order to formulate the downtime costs model for IT companies.
The interview contains three main parts: IT infrastructure, IT infrastructure interdependency, and IT downtime costs.

1. *Can you briefly describe your background?*

2. *How important is IT infrastructure for your company?*

3. *Do you have an idea about how your IT budget has been changing over the past couple of years?*

4. *Can you tell some underlying downtime threats?*

5. *How do these threats affect the IT infrastructure? Can you give some examples?*

6. *How often does the downtime happen?*

7. *Have you ever experience the downtime? (if yes, what factors causes the downtime? how does it affect your work? how long does it exist? How does the company fix it? How much money does the company loss?) What do you do during downtime?*

8. *What are your concerns from downtime?*

9. *When downtime occurs, is there any mitigation strategy?*

10. *Have you ever heard any preventive maintenance that your company adopt?*

Concluding the interview
Summarize key points provided by interviewees
Is there anything interviewee would like to add?
Ask whether the interviewee is interested in the end results of my research?

Appendix D: company profiles

Inter-viewee	Position	Work years	Work years in target position*	Industry	Company location	Company size
1	Hardware after-sale consultant	8	2	J62 - Computer programming, consultancy and related activities	Xi'an, China	Around 150 employees
2	Software engineer	4	1	K - Financial and insurance activities	Xi'an, China	Around 30 employees
3	iOS developer	2	0.3	N79 - Travel agency, tour operator and other reservation service and related activities	Beijing, China	More than 1000 employees
4	Product manager	0.5	0.5	J62 - Computer programming, consultancy and related activities	Shenzhen, China	More than 2000 employees
5	Payment security consultant	2	2	K - Financial and insurance activities	Hangzhou, China	Around 3500 employees
6	Logistic operator	0.5	0.5	H - Transportation and storage	Hangzhou, China	Around 500 employees
7	Computer incidence solver	25+	25+	J62 - Computer programming, consultancy and related activities	Utrecht, the Netherlands	Around 100 employees
8	Security consultant	16	16	K - Financial and insurance activities	Amsterdam, the Netherlands	Around 65,000 employees
9	Clearing counter	2	2	K - Financial and insurance activities	Beijing, China	Around 25 employee
10	IT infrastr-ucture manager	23	2.5	P - Education	Utrecht, the Netherlands	Around 1,700 employees

Appendix E: interview notes

Interview notes are removed due to confidentiality reasons

Appendix F: Code book

Main code	**Sub-code**	**Participants that named it**
Background/job character	management related experience	5, 9
	IT related experience	1, 2, 3, 4, 6, 7, 8,10
The importance of IT infrastructure	Information sharing	1, 3, 4, 6, 7, 8, 9
	Efficiency	1, 2, 3, 4, 6,
IT budget changes	Increasing	4, 9
	Decreasing	8, 10
Downtime threats	Natural disaster	
	Hardware failure - Outage of core switches	1, 4, 6, 7, 10
	Software failure	1, 2
	Human error	8, 10
	System overload - inter-system asynchronous communication network timeout	2, 6, 8, 9
	Virus/attack	8, 10
	Loss of network connectivity	5, 9, 7, 10
	Power outage - Circuit problem	1, 3, 4
	Vandalism - Accessing restricted files	2
	Information leakage	2
	Maintenance -Misconfiguration - System development reboot	6, 7
Concerns	Data	1, 2, 3, 6, 9
	Troubleshooting	1, 10
	Report downtime	5, 10
	Work plan	3,
	Network connectivity	2,
	Customers	5, 7, 9
Mitigation strategy/action	Backup data	1, 3,
	Soothe customers' feelings	5, 9
	Backup system	1, 6

	Stop attacks	10
Preventive strategy/action	Backup data	1, 8
	Backup power supply equipment	1,
	Extra circuits	1,
	User classification	2
	Update system	2
	Antivirus software	2, 9, 10
	Maintenance	2, 3, 9
	Monitoring	5, 7,
	Set network authority	4,
	Prior tests	5, 6, 8,