TURUN KAUPPAKORKEAKOULU
Turku School of Economics

WEIGHING THE VALUE OF CONTINUITY MANAGEMENT

Analysis of disaster recovery planning in organizations

Master´s Thesis
in Information System Science

Author:
Danish Islam

Supervisor:

Dr.Sc. Jonna Järveläinen

25.9.2010
Turku

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

- Continuity management planning (CMP)
- Continuity management (CM)
- Disaster recovery planning (DRP)
- Global innovation technology management program (GITM)
- Business continuity planning (BCP)
- Business continuity management (BCM)
- Recovery time objective (RTO)
- Recovery point objective (RPO)
- Business impact analysis (BIA)
- Security risk management (SRM)
- Denial of Service (DoS)
- Spamming (SPAM)
- Multi-protocol label switching (MPLS)
- Maximum tolerable period of disruption (MTPD)
- Service delivery objective (SDO)
- Information system security (ISsec)
- Information security (IS)
- Confidentiality integrity availability model (CIA)
- Mission business task critical (MBTC)
- Chief information security officer (CISO)
- Information security/system manager (ISM)
- Information technology service manager (ITSM)
- Information communication technology manager (ICTM)
- Risk compliance officer (RCO)
- Head of security Finland (HSF)
- System manager (SM)
- Chief information officer (CIO)

1 INTRODUCTION

1.1 Research topic and motivation

The topic of continuity management depicts an important phase in the field of information system security (ISsec) and the growing importance in terms of its implementation and application. Disaster recovery planning is part of the continuity plans that is becoming the ISsec standard in not only IT companies, but business giants of the world today as well. It provides a company a form of assurance in time of crisis and can be the difference between them surviving an incident or not.

Businesses nowadays are required to operate on a 24 hour, 365 days a year time frame. Even after the occurrence of an interruption, a company has an average of 24hrs to two days to come back to normalcy to stay afloat according to Noakes-Fry (2001, 2).

Along the same theme, there is a lack of ISsec research on an organisational level and this leaves a gap between the understanding of business continuity management (BCM) and issues like disaster recovery planning (DRP). This void needs to be addressed by a more specific and concise study of the BCM discipline and hence it is extremely important for the firm to be viable and resilient in order to survive (Kotulic & Clark 2004, 605).

Moreover, business continuity management (BCM) has moved rapidly up the boardroom agenda. Just a few years ago it barely featured on the agenda at all. September 11 and other incidents and disasters - both natural and man-made have meant that it has assumed a much higher profile. It should be a real concern of the board and of the audit committee (Gallagher 2003, 15).

A Computer World magazine article (2006) in the security log column, “Tech Companies found to be Lax”, argued that technology, media and telecommunication organisations neglected to give enough funds and resources for security even though they had had a security breach over the past year, which was a research conducted by Deloitte Touché Tohmatsu (Computer World 2006) . This provides motivation to study and research the area and find out the conditions in Finland.

Companies cannot ignore the agenda nowadays and furthermore, the research to understand continuity management planning in companies in Finland, would give an excellent opportunity to analyse the issues of continuity management and disaster recovery in organizations in the country.

1.2 Research questions

With this research, we try to understand the situation of continuity management planning in Finnish companies. In order to be clear on the research topic, the main research problem of this thesis is the following:

What is the importance of continuity management planning in companies?

Looking at this main research question, there is an element that needs clarification. The term continuity management addresses companies and businesses and this leads to further questions regarding continuity planning, what is the status of business continuity management? To clarify the main question, sub-questions could be formed to divide the main question as follows:

1) How is disaster recovery managed in companies?

This question breaks down the main question in to the DRP. This plan is discussed in chapter 3 of the literature and examined in detail from the interviews of medium and large companies and compared to the literature itself and the question is then answered.

2) What is the state of disaster recovery planning in companies?

This question further examines this plan in companies and the status of this plan is identified after conducting the interviews and the results are realised in accordance with the literature review as well on this topic from chapter 3.

3) What is the best practice in companies when it comes to dealing with continuity management and disaster recovery?

This question examines the defined concepts in these plans in the literature review discussed in chapter 2 and 3 and then the 'best practices' of companies are studied from the interview case study and compared to the literature again answering the question in turn.

4) What is the status of BCM in companies?

Chapter 2 discusses BCM in detail and the literature together with the interviews is used to examine the status of BCM in the form of how companies respond to disaster and crisis situations. The interview findings in chapter 5 are compared and linked to the literature and aimed to answer these respective questions.

The situation of continuity management in Finland is analysed since it is found out whether companies perceive it as important or can they function without these plans. These in turn will help to understand the present situation and give concrete information

concerning the importance and existence of these plans in Finnish companies. With this research problem, and the sub questions, the current situation of continuity management in Finland is potentially clarified as there is a lack of research according to Kotulic and Clark (2004, 605) on this issue.

2 BUSINESS CONTINUITY MANAGEMENT

To understand the state of continuity management in Finland we must first discuss and find out what different literature exists regarding the topic of business continuity management and start off by defining the concept, then discussing the link to ISsec and finally the need for BCM itself.

2.1 Definitions and brief history

Getting straight to the point, we start off with brief definitions of business continuity management and according to Gallagher (2003, 15), business continuity management (BCM) is now being involved in all aspects of a company, not just IT.

The Business Continuity Institute (BCI) defines BCM as “the act of anticipating incidents which affect mission-critical functions and processes for the organization and ensuring that it responds in a planned and rehearsed manner.”

This definition emphasises three key constituents, Gallagher (2003, 15)

- “It is the act of anticipating incidents”: The organisation at hand must examine the risks and security issues it is exposed to and consider how to manage them in a considerable manner if they should occur.
- “Which affect mission-critical functions and processes”: BCM is not merely a plan or procedure that is utilised when an incident occurs for example a security breach; it is concerned with major threats and issues that have a direct impact on the core activities of the company. The documentation of procedures of failures for daily processes must indeed exist but BCM must emphasize the bigger organizational picture.
- “Ensuring that it responds to any incident in a planned and rehearsed manner”: This element of the definition involves the planning, the complete attention of the right personnel, acceptance and ownership of the agenda and a stern test of all significant prerequisites of the correct and satisfactory response.

According to British standards institute (2006), BCM is now defined as "an holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities". This definition stems from the BS25999 standard which is the corner stone for professional standards today in IT security management.

According to Noakes-Fry (2001, 3), business continuity management is a plan that exists throughout the organization consisting of the strategic framework stating various

tactics to mitigate risks that may cause business process failure, asset loss, regulatory liability, customer service failure or damage to brand image and reputation.

All these definitions provide explanation on the importance of BCM and what it helps the company to achieve in the case of disruption, Gallagher points out that it enables the organisation to remain functional and Noakes-Fry mentions its importance in the way of a strategic framework that mitigates risks and finally, the definition by BSI, makes BCM a very useful tool to identify potential dangers and makes organisational processes resilient, and capable of responding to disruptions of all kinds and maintaining security of assets and reputability. In light of the definitions stated dealing with the subject of business continuity management, similarities lie in the fact that they all discuss risk management, or some kind of mitigation of the threats the organisations face. There are dissimilarities as well between them as in the first definition by Gallagher (2003, 15), there is the act of anticipation involved; the second discusses the organisational framework for business continuity management and finally, the third definition is a shorter version of the second with the difference that it states that business continuity is a plan. The most appropriate explanation for the purposes of this research stems from the one by British Standards Institute (2006), the second definition. The reason for this choice is straightforward since it recognises the plan with respect to management strategy, business operations, and risk management all in accordance with the framework of the organisation. The link to the research question can be seen in the definition by BSI (2006) as well. It describes it as a management process that enables a business to be resilient and respond to those threats. Looking at the main research problem, “What is the importance of continuity management planning in Finnish companies?”, we find the alignment with the complete framework of continuity management, including all ISsec and disaster recovery processes as well and this is found in the definition by the BSI as mentioned.

2.2 Information security aspects and business continuity management

Companies have been reluctant in the past to reveal information about critical events and security measures according to Kotulic and Clark (2004, 605), and probably the best information about business disasters and continuity and recovery projects is locked away in the depths of company's filing cabinets (Toigo 1989, 201).

Moving into the thematic framework, Nollau (2009, 51) states an important fact about business continuity management that if one wanted to find out how disaster recovery and business continuity really work, they have to go to Puerto Rico due to the numerous hurricanes their IT teams in companies deal with annually. The following diagram (figure 1) generalises an organisation and the relationship to business continuity and disaster recovery planning. It shows that all functions or departments of organisations become more resilient and robust by incorporating continuity management. Business continuity management (BCM) is the core and it involves the business continuity plan (BCP) and this plan incorporates the disaster recovery plan (DRP) and information security (ISsec) policies as well as shown in figure 1. The departments shown rely on BCM in time of disruption to continue to function, departments or functions of organisations as management, human resources, production, marketing, logistics, research and development and IT even.

Information owned by companies today is increasingly being used by not just employees but customers and partners as well and they expect non-stop availability and access to this information if the company is to keep a competitive edge. From the organisation's perspective it is only possible if it manages to keep the information confidential, accurate and continuously available. With respect to BCP, ISsec aspect is the availability feature of the information (Botha & Von Solms 2004, 329).

In general, information security is the basic implementation of policy that ensures confidentiality, integrity and availability (CIA) of any kind of information or asset or anything that is of value to an organisation according to Smith & Jamieson (2006, 25).

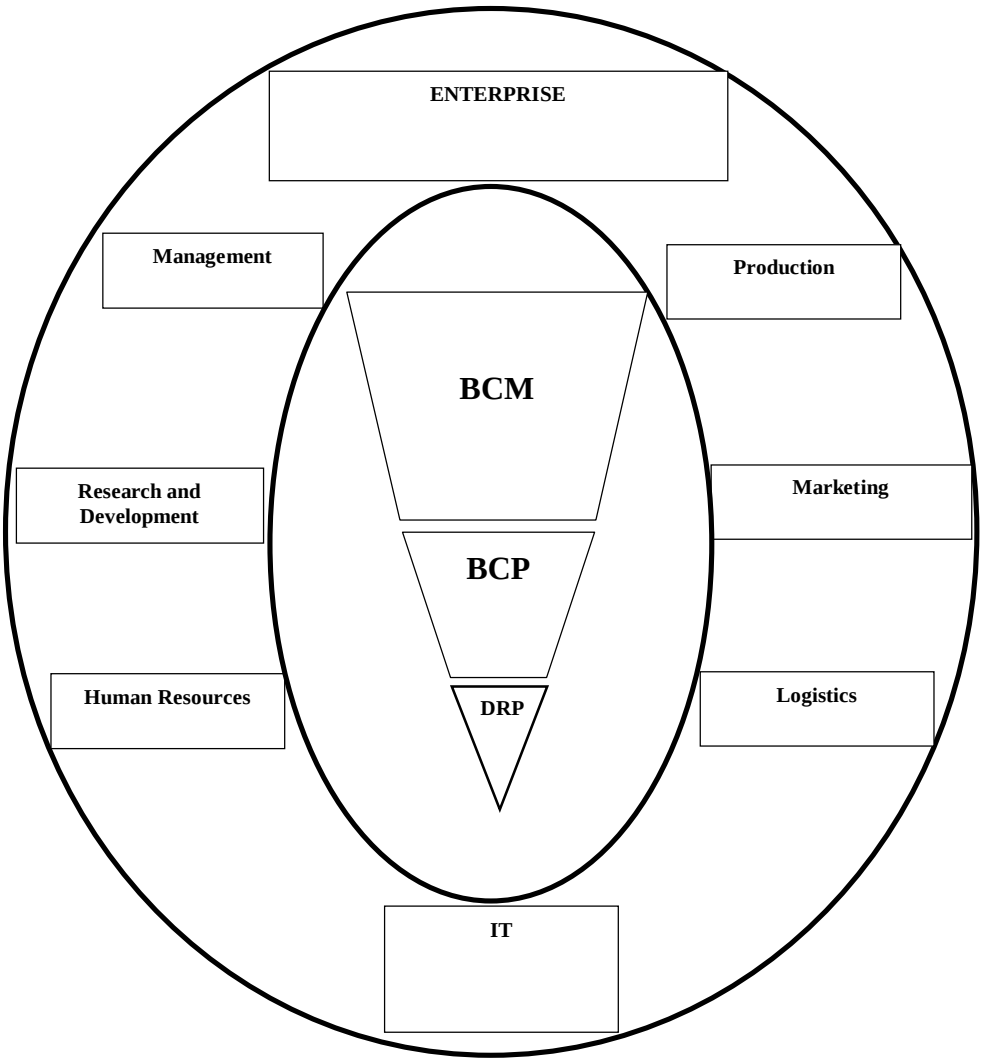

Figure 1 Generalised model of an organisation showing relationship between continuity management (Adapted from: Nollau 2009, 53).

More specifically, the objectives of information security are to preserve an entire company's information asset and the business functions and processes. Confidentiality is considered as ensuring that information is only available to the people that are authorised to receive it. Then, the integrity comes into play which is ensuring of information alteration again only by those authorised to do it and finally, availability means the ensuring of information and the systems that process and handle this information are available when needed. These objectives have originated from all kinds of security standard bodies like OECD (organisation for economic cooperation and development), BSI, ISO/IEC and such through the 1990s. Since organisations have to work around the clock as mentioned earlier by Noakes-Fry, a disaster affecting them can be minimised by contingency planning and this involves the creation of the business

continuity plan (BCP) as shown in figure 1. The BCP is incorporated in the business continuity management which has been defined earlier by BSI (2006). The BCP should cover the following:

- Planning for continuation of business functions when disaster strikes.
- ensuring that critical business functions are restored as soon as possible
- focusing on prioritised resumption of these critical business functions,

A BCP is a significant constituent of IT security in a generalised form and ISsec in particular (Smith & Jamieson 2006, 25). This link between the organisations, ISsec and continuity management steers the research and helps in understanding the value of business continuity management and disaster recovery. For the purpose of this research, BCP encompasses DRP and ISsec and they are elements of the BCM.

The basic components of the BCP are argued to be the business impact analysis (BIA), all the contingency and recovery plans and the testing and updating of the BCP itself that checks to see if the plans actually work, and whether the people involved actually know what to do when a disruption occurs; testing under more real conditions so confidence increases and panic is avoided. The BIA (business impact analysis) identifies the critical functions that the organisation must perform to remain functional and stay in business altogether, then it identifies risks to these critical functions and rates those risks in accordance with probability of it actually happening and finally, it suggests the avoidance and mitigation of risks (Cerullo & Cerullo 2004, 71).

It is important to consider the development and maintenance of business continuity planning which is of high priority today due to the growing number of threats to companies, natural or man-made, and the present lack of governance benchmarks (Sheth, McHugh & Jones 2008). The components for the framework of business continuity can be seen in figure 2 which can be considered as an explanation of the middle section of figure 1.

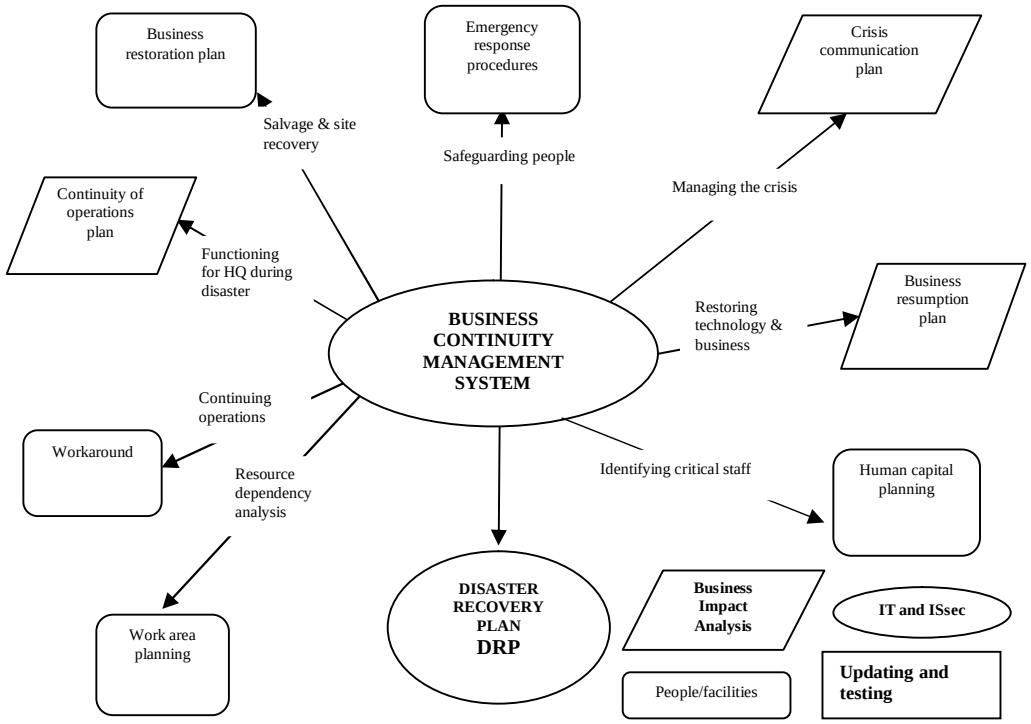

Figure 2 Components of Business Continuity Management (Adapted from: Sheth et al. 2008, 225).

This is an important illustration of a business continuity system and explains in detail the constituents of BCM and all the processes to maintain organisational information security. It is basically an elaboration of the BCM component from figure 1. This figure contains all the plans, the initial plans when a disaster strikes to the completion of restoration of a business. Many established businesses go through the following phases or stages in the case of a disaster today together with their respective response plans, these sub-plans are components of the following four plans in business continuity management (Sheth et al. 2008, 225):

- Response (right after disaster): Emergency response plan and crisis communication plan
- Recovery (IS/IT focus mainly plus workarounds): Resource dependency analysis and workaround plan.
- Resumption (recovery of businesses processes dependant on IT): Disaster recovery and business resumption and continuity of operations plan
- Restoration (normalcy after the event of disaster): Business restoration plan.

The emergency response plan is designed to protect the lives of staff and employees in the company immediately after a disaster and the crisis communication plan manages the public relations aspect of the organisation (in terms of company image) such as a

laptop battery exploding and so on. Then there is the ‘recovery plans’ and these identify the infrastructure needs together with the workaround plan that allows the business to function from the point of disruption until the completion of recovery. Then there is the ‘resumption plan’ which contains disaster recovery plans and business resumption plan. DRP constitutes recovery of IT processes and functions and recovery of critical business processes. Finally, the ‘restoration plan’ deals with the salvaging and recovery of the site and returning to normalcy of processes and operations of the organisation. Their names can be different across companies but the essential content and processes involved are the same (Sheth et al 2008, 225).

Information security constitutes the CIA, confidentiality, integrity and availability model mentioned by Smith and Jamieson (2006, 25), which falls under the business continuity management function in an organisation as argued above. Information security in turn has been addressed in different ways that involve a technical design of security systems and policies and also in other fashion that involves a more socio-technical approach to the topic (Anderson & Agrawal 2010, 616). Since the research topic involves continuity management and disaster recovery, the technical aspects of ISsec will be considered.

According to Gibb and Buchanan (2006, 140), business continuity management is essential in protecting the enterprise/business from its environment. The CIO (Chief Information Officer) has to make sure that both information management and the philosophy of BCM is in place to mitigate and mediate recovery in the case of an interruption and have contingency plans to avoid loss of revenue and stoppages in core business functions.

These particular cases described above provide examples and illustrations of the framework for business continuity management. Figure 1 describes the general organisational dependency on BCM and what it comprises of in terms of BCP and ISsec and DRP (Nollau 2009, 53). The second figure shows the business continuity management system in a comprehensive manner (expansion of figure 1) and depicts the entire plans linked to continuity constituting the disaster recovery plan, the emergency response plans, the continuity operations, workaround plan, crisis communication plan, restoration plan and resumption plan (Sheth et al. 2008, 225). From these figures and literature, the ISsec process has been placed in the BCP function of an organisation and the links it forms is the overall value it creates for the organisation when these plans exist and ISsec ensures the security together with BCP. There is a need to build a framework for the plans that constitute what should ideally occur or how the business can be assured in case of a disaster and information security ensures that the right people handle the right information at the right time in managing that disaster. Figure 1 and Figure 2 provide comprehensive illustrations of a BCM (within the organisation and all the plans it contains) and they are strengthened by ISsec policies that exist in a

company (Smith & Jamieson 2006, 25).

The definition of BCM also can be linked here (BSI 2006) as well as it was described as “a holistic management process”; according to figure 1, it was indeed the case as BCM was the core of the entire enterprise, “which identifies potential threats and impacts to an organisation”; this part is identified with the BIA, ISsec and CIA model of information handling and then “the framework for building organisational resilience to enable an effective response”; is found in all the plans described by Sheth et al..

The research questions can be linked here since we have seen the components of a BCP, and can reflect upon the sub-question on the status of BCM with these plans in mind and what value they would bring to an organisation.

2.3 The need for business continuity management

Going back some years ago, keeping in mind the disastrous effects of September 11 and the World Trade Centre, directors and senior managers cannot ignore the consequences if a business continuity plan is not in action (Herbane, Elliott, Swartz 2002, 224).

Disruptions caused by power outages, floods, snowstorms and other external cyber-attacks (DOS attacks, viruses, phishing, spam etc.) or internal leakage of critical information can occur and cause downtime which can cease business critical functions of organisations that are sometimes even irreversible. This is the reason it is critical for organisations to render BCM a major factor in operational and managerial strategy as well (Sheth et al 2008, 223).

Numerous examples are found where business continuity planning and management have been utilised and in the article by D’Amico (2007, 220) it is argued that there is more concern about major disasters and not enough thought given to ‘daily’ breaches and disruptions, equipment problems and information theft. How the company reacts to these scenarios will indirectly or directly affect their growth at least in terms of market share and public image. In 1982 Johnson and Johnson pulled Tylenol capsules from the market due to a product defect and did not wait for any more information about the defected item hence they did not try to buy any time so to speak to assess the damage. Once the fault was assessed they made the package tamper-proof and re-launched it. This had an amicable effect on the brand and it did not lose its image and further strengthened Johnson and Johnson as a customer-first organisation (D’Amico (2007, 220).

Another example that focuses on the negative impact the lack of BCM comes from USA at a candle wax manufacturing plant where they had a fire breakout and lost the entire building plant and although there were effective and efficient backups done on computer systems, which were onsite. Hence all tax and crucial details such as

manufacturing, vendor information, customer names and important formulas for scented candles and so on were lost in the blaze (D'Amico 2007, 219).

Table 1 identifies the three phases of BCM with respect to disaster recovery according to D'Amico, namely resolve, respond and rebuild.

Table 1 Three phases of BCM (Source: D'Amico 2007, 215).

Resolve	***Respond***	***Rebuild***
Identify roles and responsibilities	React quickly	Assess the damage
Document mission critical processes	Engage public emergency response services	Manage the insurance claims process
Catalogue important assets	Notify internal responders and other key contacts	Engage external resources
Define key contacts	Take steps to minimize and contain the damage	Bring replacement equipment online
Evaluate risks	Stabilize the situation	Communicate the situation and the plan
Take pre-emptive actions	Contain the fallout	Expedite the return to normal

As seen before in Sheth et al.'s illustration of BCP which had four plans, response, recovery, resumption and restoration to be specific, D'Amico shows some similarities as the article includes "resolve", "respond" and "rebuild" phases. He discusses them as phases instead of plans and contains the respond phase that mentions "react quickly" and "engaging public emergency response" phases which are similar to the response plans by Sheth et al.; the response phase that included the emergency response plan and crisis communication plan, and D'Amico mentions notification to internal responders and key contacts which makes it similar to the response plan discussed by Sheth et al as that discussed the public communication/notification as well. The rebuild phase is similar to the restoration plans by Sheth et al. since it contains the return to normalcy of processes and functions of the company. D'Amico shortens the resolve phase that was mentioned separately by Sheth et al. as recovery and resumption plans. Additionally, D'Amico mentions evaluation of risks and documentation of mission critical processes which is different from the recovery and resumptions plans since they contained specific resource dependency and workaround plans in the recovery plans and DRP and continuity of operations in the resumptions plan. Hence it can be concluded from this comparison that Sheth et al. discusses a more comprehensive framework of BCP.

Further assessment of these disruptions allows for an impact analysis and this is shown in table 2.

Table 2 Impact levels and disruptions (Source: D'Amico 2007, 218).

Impact	***Minimal***	***Moderate***	***Major***
Business interruption	Little, if any, customer or revenue impact	Some customer or revenue impact but manageable	Significant impact on revenue and customers
Customer service and support	Little, if any, customer impact	Some customer impact but manageable	Significant impact on multiple customers
Casualties	None	Some injuries but no deaths	Multiple injuries and deaths
Property damage	Slight	Confined to one area	Several areas impacted
Community impact	None	Community expresses concern though the impact is limited	Surrounding community is adversely affected
Media attention	None	Some local media calls for information	National attention
Communications effort	Few, if any, announcements required	Internal announcement required and, possibly, a public statement	Internal, public and individual customer announcements required
Management intervention	Easily managed by middle managers	Some senior management attention required	Deep involvement by top managers and board members

Table 2 deals with the level or impact of the different disasters that have affected businesses and the response required accordingly. It is shown that disasters or disruptions can have different levels, minimal, moderate and major and should be dealt with the measures specified. The impact column represents the kind of disruption and depending on the corresponding level, the response is generalised. Business interruption can have the slightest effect under a minimal circumstance, and a critical impact on the maximum scale. Customer support disruption could be moderate but manageable as shown but a major disruption to customer service and support could have a significant bearing on the major scale. Casualties are obvious causes in terms of major disasters and the lighter side in a minimal disaster would be no casualties. Property damage could be none to several areas impacted by major disaster. Community impact is none in the

minimal case and in the major scenario; the community would be severely affected. Media attention is none in minimal case, some local media in the moderate one and national and international attention is required in a major scenario. Communications effort on part of the company involved would be minimal for a trivial disaster, internal communication would be required for a moderate disaster and a public and internal along with the customers involved individual would have to be notified. Management intervention in a company handles the disasters in different way, a minimal disaster could be handled by the middle managers themselves, a moderate one should involve some specific team or senior management and a major disaster would involve deep involvement of the board members and senior management (D'Amico 2007, 218).

There is a link to research questions here since we acknowledge that these disruptions are part of every company so it is inevitable that they will go through some kind of disaster on these levels and mentioned and explained in table 2. The main question, "what is the importance of continuity management planning in Finnish companies?" can be addressed by the examples of disasters mentioned in table 2, such as business interruption or customer service and support as these signify a scale of a minimal effect until a major catastrophe for the business, and thus, it's importance is validated since the BCP will consider these situations in the company and take care of the important assets as mentioned in the definition (BSI 2006).

In the article by Ross and Weill (2002, 89), there are examples of state of the art high end enterprises that can afford no downtime, like the US state lottery company GTECH Corporation, or Merrill Lynch. These companies do not compromise on any end to protect critical information. There is a realization that not every company needs such a recovery system as the aforementioned example of GTECH Corporation because of the simple fact that it might be too costly for them to have such recovery systems such as mirroring and so on.

A 2008 survey by UK Chartered Management Institute demonstrated that 76% of managers stated that their senior or top management regarded BCM as crucial to the company's operations and strategy, only 47% of these companies had a BC plan in place (Seow 2009, 201).

According to Seow (2009, 201), top managers need to be motivated and CIO's or IT managers must gain complete backing of top managers in order to enhance, sustain and even implement a BC plan. Commitment and buy-in are keys for successful programme. It is argued that BCM is a relatively new discipline, and it is important to clarify what it is and there is a need to continually raise the awareness and recognition. Therefore, the BCM programme needs to be viable and an on-going system, showing the value of having and sustaining it is extremely important in companies today due to the ever challenging environment.

In harmony with businesses, finance (department) has their BCM concerns as well.

Business interruptions, which can occur on a monthly, quarterly or yearly basis, hinder filling and financial reporting in businesses. There has to be collaboration between finance and IT about the cost of BCM system and service. Finance (department) plays a major role in providing the level of protection the business unit needs (Krell 2006, 28).

The need for business continuity management cannot be overlooked and it would be a shame if an organisation that had the capability to survive did not do so due to lack of appropriate business continuity procedures. The ability of BCM to resolve and sustain a business has become a major boon for companies and there is no room to omit and undermine the concept since it brings tremendous potential to all functions of the organisation: the strategy function (identifying the critical business functions and recovering them), financial (provide cost cutting solutions to organisation with IT infrastructure management), operational (identify changes in business environment), infrastructural, legal and staff oriented functions as it covers these tasks in the recovery plan as is argued in the articles and examples (Bandyopadhyay, Mykytyn & Mykytyn, 1999, 225).

On a summarizing note, looking at these examples of business disruptions, the levels and the ability to respond, resolve and survive them has been the most important aspect in all kinds of organisations (D'Amico 2007, 215). The examples above such as the candle wax (D'Amico 2007, 219), GTECH Corporation (Ross & Weill 2002, 89), SARS outbreak (Sheth et al. 2008, 223) and the September eleven tragedy (Dominic et al. 2002, 224) has shed light that the accurate handling of the situation is very important for organisations for ISsec risk mitigation.

These examples and arguments provide significant weight in the case for BCM's value in organisations and we can link to the sub questions as well from the continuity planning and BCM status questions when it comes to Finnish organisations and research can be conducted to show what exactly is the situation with BCM and continuity planning, how are they considered in the local businesses'. The following chapter deals in depth with the integral IT part of BCP, the DRP.

3 DISASTER RECOVERY PLANNING

Rolling along the issue of continuity management, the IT aspect of business continuity management has to be discussed. As found from the preceding literature, the integral plan in BCP is the disaster recovery plan. This chapter discusses literature on DRP's history, its value and its importance to organizations concluding with a formulation of a framework that is derived from this together with the previous literature on BCM.

3.1 History and literature on disaster recovery plan

Having developed an understanding of BCM, we now switch to the core topic DRP which is turn part of the BCM plan. DRP deals with recovering mission-critical technology and applications at an alternate site, to put it in the simplest of words (Noakes-Fry 2001, 3).

It can be a form of document in many cases that is designed to aid in the process of data recovery and other losses of data assets. Disaster recovery was initially a term coined by IT security specialists in and around 1960-1980 and during that time it was mainly a disaster recovery for mainframes (Hawkins, Yen & Chou 2000, 222).

To make an accurate account of disaster recovery plan, we need to acknowledge the fact that BCM encompasses the BCP (Business continuity plan) and DRP, when, there is already confusion about the two terminologies. It is an unfortunate fact that in many organisations, IT security and risk management is carried out as two independent operations or modules as is their business impact analysis (BIA), therefore they are not linked, which in turn causes these organisations to ponder on what IT services and security issues are tied to the business processes and which to recover, resolve and respond to when a disaster strikes (Bhavani 2010, 5).

This is contradictory to the previous classification of DRP which came under the BCP and BCM was the overall umbrella, as discussed earlier (Smith & Jamieson 2006, 25). It was argued that DRP would fall under BCP but we cannot refute the possibility of different models existing; hence it is important to include Bhavani's argument here.

Following is an illustration of the companies in US that went out of business and could not recover from disaster with respect to time. A period of 1, 3 and 5 years with respect to data loss or other disaster is notified here. It depicts an impact of the disaster and the companies that do not recover or suffer due to lack of DRP (Bhavani 2010, 5).

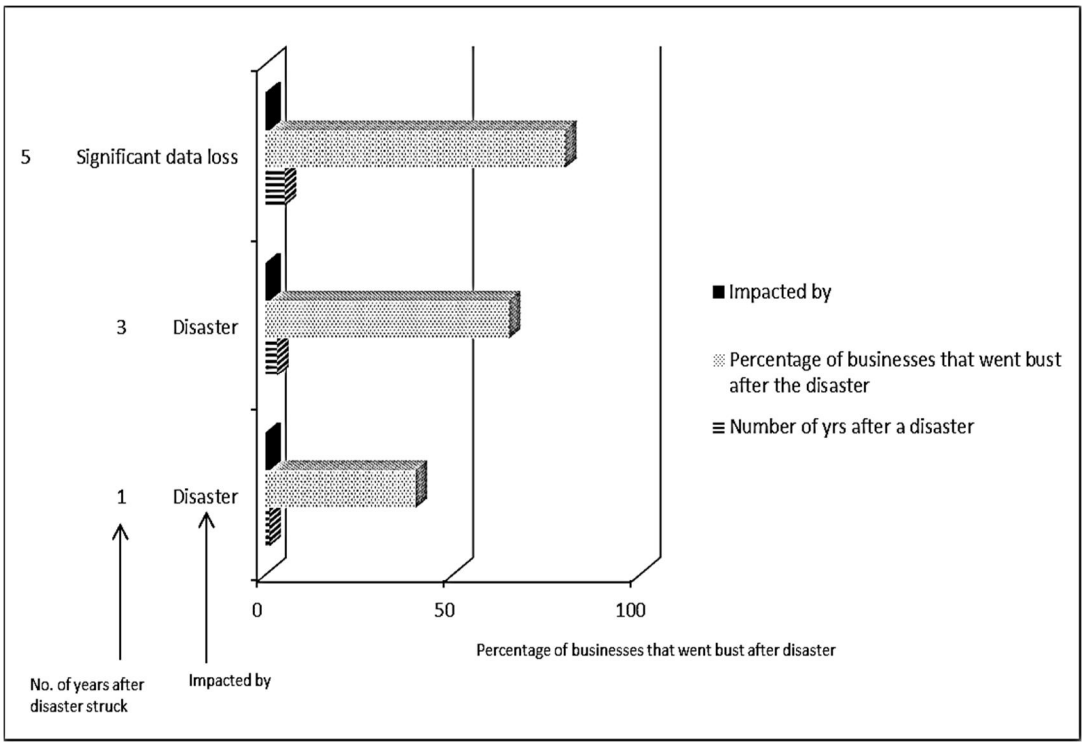

Figure 3 Impact analysis of disasters (Source: Bhavani 2010, 5).

As shown in the finding here, it is astounding that so many companies do not recover in time from disasters if they do not have an adequate DRP in place. Moving over from academic or scholarly journals and switching to CISA Review manual 2007 version (Certified information systems auditor), a professional perspective on disaster recovery planning with regards to what is being used as the common practice and standards is also considered. BCP includes the DRP, the operations plan and the restoration plan. IS DRP takes into account the ISsec processes and contains, or should contain the policy of recovery processes of IT and security infrastructure to make the damage minimal. The processes linked can be shown in the diagram below which depicts the life cycle of the BCM or BCP:

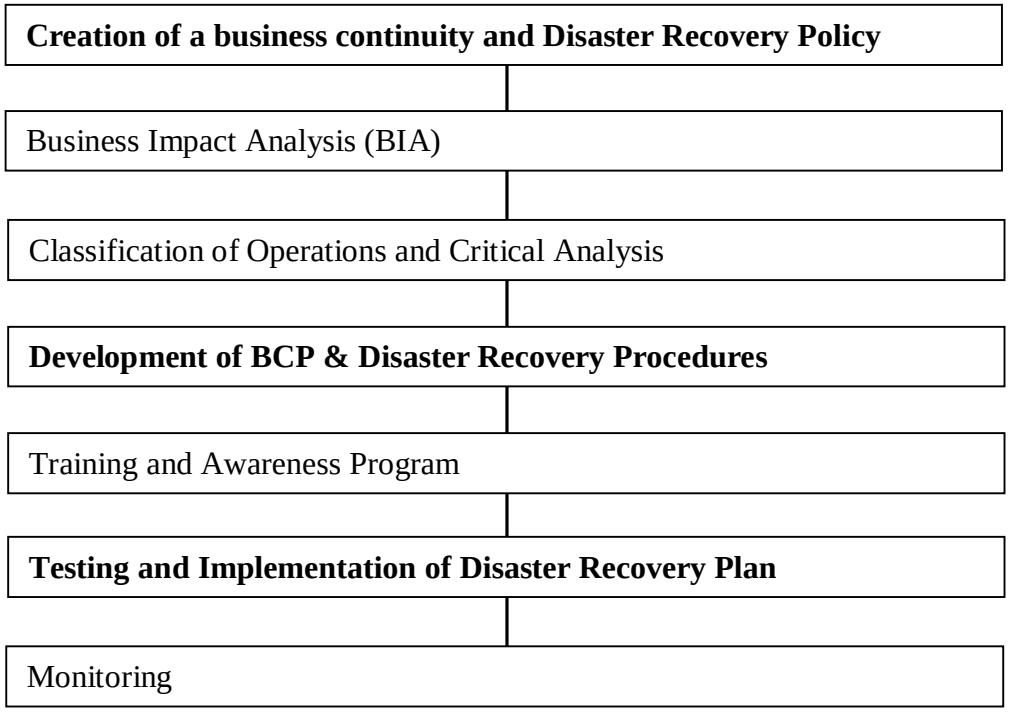

Figure 4 The Business Continuity Process (Source: CISA Review Manual 2007, 447).

From the cycle above in figure 4, it is evident that after BIA (Business Impact Analysis) and critical operations are identified; the disaster recovery plan is formulated based on RPO (Recovery point objective) and RTO (Recovery time objective). These RPO and RTO are illustrated to give a better understanding in figure 6. These two metrics aid in identifying the recovery strategies to be used in the DRP. Therefore, to come to that phase where disaster tolerance for certain processes can be accepted gives a clear understanding of the procedure with respect to time. The business impact analysis (BIA) is a critical phase in the establishment of the disaster recovery plan. This phase results in the identification of various events that could have a potential impact on the daily business operations, such as the finances, the human, the important business and strategic functions and the technological and reputational impact these would have in the company. The organisation basically asks itself during the determination of these functions, the following questions, what are the different business processes based on needs and relative importance? What are the critical or not so critical information resources related to the company's critical business processes? These could be production, receiving payments, legal and regulatory compliance or revenue management. Finally, what is the critical recovery time period for maximum tolerable disruption? (CISA Review Manual 2007, 449-452).

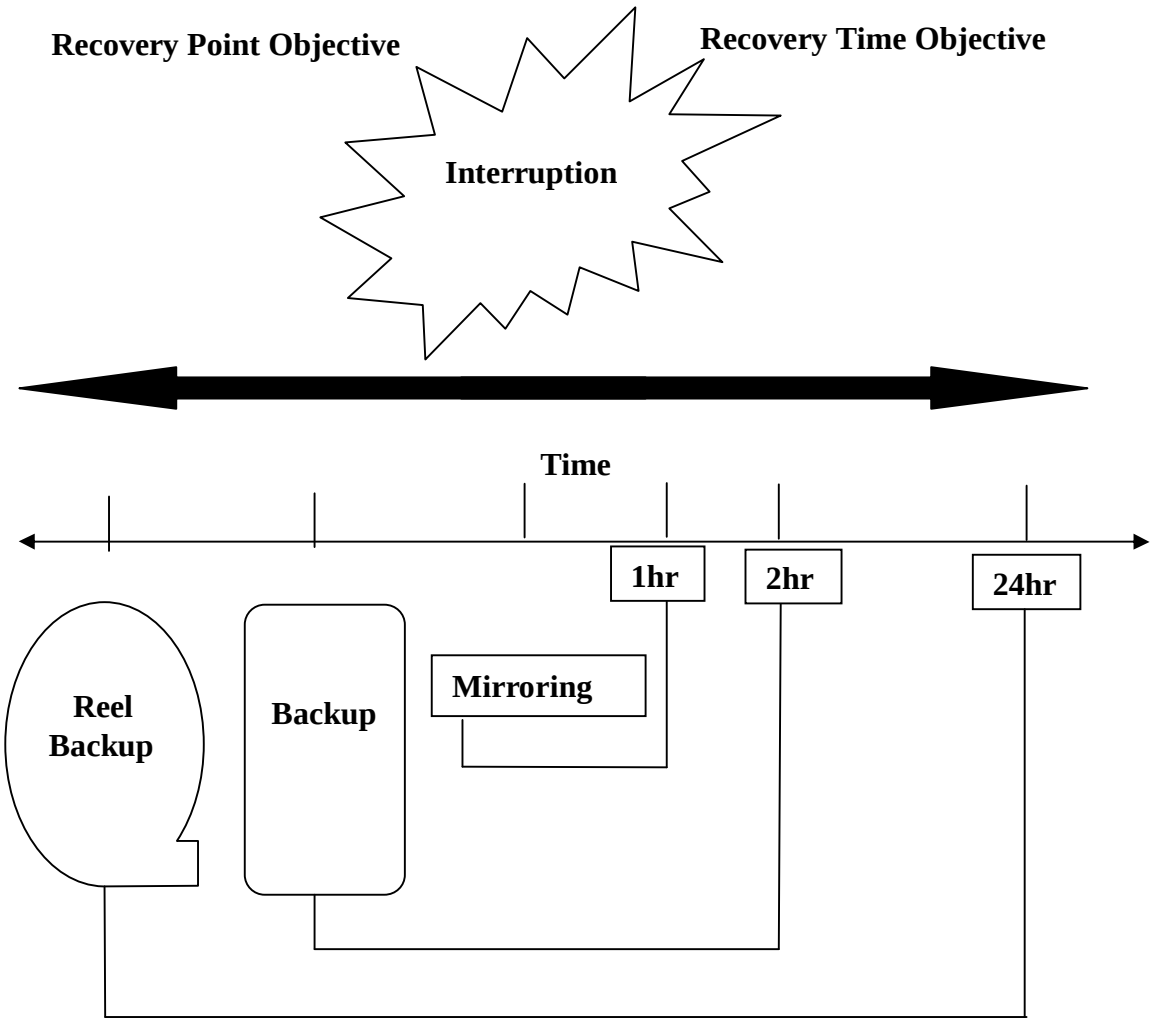

Figure 5 Relation between Recovery Point Objective and Recovery Time Objective (Source: CISA Review Manual 2007, 452).

In addition to RPO (recovery point objective) and RTO (recovery time objective), sometimes companies utilise service delivery objective (SDO) which is directly linked to business needs and encompasses the alternate process that run until normalcy is achieved. Furthermore, maximum tolerable outages (also known as maximum tolerable period of disruption, MTPD) and interruption window (the time an organisation can wait before the disruption of the process and functionality becomes unaffordable) are modules that bear significance in defining the DRP. The recovery point objective indicates the earliest point in time that a data can be recovered and this hence deals with the acceptable data loss. For example, if a process can allow data to be lost for up to 3hours, then the latest backup should be available for up to 3hrs before the disruption. The recovery time objective is dealing with the acceptable downtime in a process or function. This is an indication of the earliest point in time that a business operation must resume at any cost after disaster or disruption. These are shown in the figure 5 (CISA Review Manual 2007, 453).

Based on the inputs from BIA, the critical analysis and recovery strategy selected by management, the disaster recovery plan should be developed. It is thus constituent of the entire period of disruption to the point of recovering from the disaster.

Some companies cannot afford a single 24hr period for downtime, for example some financial and insurance institutions or banks. Hence we see the mirroring option in the figure 6 above which, according to Xiao et al. (1999) is very expensive replication of the entire hardware and communication facilities for companies that can afford it (CISA Review Manual 2007, 457).

The plan should be documented in simple understandable language and cover the following aspects:

- Pre-disaster readiness (incident response management)
- Evacuation or relocation details
- Recognition or declaration of disaster
- Situational importance of declaration of disaster, for example a virus attack might be a simple threat when dealt with promptly but when not declared, could lead to business interruptions and cause serious IT security damages.
- The crystal clear responsibilities of the plan, which personnel are responsible for what
- Contract information, usually from IT security and BC vendors need to be clear and identified properly and updated
- Step by step explanation of recovery options
- Identification of the resources needed to carry out recovery and continued operations of the business-critical processes

The plan should also be preserved offsite and it is sometimes common in organisations to have specifically assigned teams for disaster recovery who carry out these tasks and maintain the security and integrity of data critical to the organisation. These are known as DRT (Disaster Response Teams) (CISA Review Manual 2007, 457).

The examples of literature on DRP and all the details that go into planning a DRP with the different inputs, the BIA, the RTO, RPO, MTPD mentioned in the articles in this section share one important fact about DRP; it is a plan to revive the technical and IT infrastructure in the company. The disaster recovery plan therefore explains the manner in which operations are to be continued after the occurrence of a disruption, and this is quite vital. It is a living and breathing plan of action(s) that is formulated after the recognition and inclusion of business impact analysis and includes the recovery time and recovery period objective metric or the maximum tolerable period of disruption, depending on the type and importance of data or process (CISA Review Manual 2007, 457).

This plan is IT based and is a more specific and technical document when compared to the other plans as mentioned earlier by Sheth et al and D'Amico as they explained the entire scope of the plans or phases, this is a more direct IT oriented plan. Going back to the research questions, "What is the value of continuity management planning in Finnish companies?", "What is the state of DRP and BCM and so on, we can acknowledge from the above explanation of DRP that it is indeed valuable to companies that want to survive a disaster and escape unscathed and figures 4 and 5 show the workings of a DRP as well. Hence, the state of DRP and situation in Finnish companies will give us a better understanding of this plan.

3.2 Value and importance of disaster recovery plan

According to survey conducted by InfoTech Research Group (US) in 2008, about 60% of businesses (SMEs) do not have concrete ISS DRP in place in the case of mild to severe disasters. Moreover, the severity of this situation is acknowledged by Faulkner Information Services who claim that 50% of these businesses go out of existence in about 24months (Chisholm 2008, 11).

The simplest reason to consider how important a DRP is actually dependant on the organisational data and information it uses. As almost all organisations deal with data or some kind of information handling, they need to utilise it, manipulate it, organize it, and store it and so on and so forth. Hence, managing information appropriately and securely would be vital since it is a 'lifeline' of an organisation. So, a DRP is indeed very important to assure that data or information is kept secure before and after an interruption, mild or severe. The recent deployment of BS 25999 Business Continuity Standard has finally started to link BCM, incident management and IT disaster recovery. Tied to the importance of sustaining a complete BCM system (as explained earlier as well by Sheth et al.), the organisation should also have an IT DR plan. Thus BCM should entail a clear and concise DRP enabling the company to cover critical IT services and security issues (Bradbury 2008, 14).

This is in line with the opinions of Toigo (1989, 233-237) and Epich and Persson (1994, 5) that DRP offers an organisation a unique assurance of its capability to handle data securely and maintain its integrity. As indicated by the previous analysis of DRP, it is actually enabling the organisation to protect its assets and even minimise data security issues, loss of customers, image and market share. There is indeed a positive correlation with the total disaster recovery in an organisation and the existence of a DRP in that organisation. In many organisations, especially those in the banking sector, DRP also helps minimise legal risks. In the US, there is a legal mandate that requires banks to

mediate and manage the risk of data loss with the obligatory presence of a DRP. The managers are held liable for lack of preparedness in these circumstances such as a bank's failure to face a disruption such as a computer outage. Also, the existence of a DRP provides a discount on the insurance premiums for business interruptions. The presence of DRP also enables firms to recover to minimal operation level in the least time possible which enhances the service level offered to customers, especially in the case of a bank leaving the customers satisfied. Even the staffs in the organisations are less stressed if they are aware of the recovery plan procedures and its functionality.

When it comes to reducing the IT and IS risks, DRP goes a long way according to Bandyopadhyay et al. (1999, 441), and managing even natural disasters as shown in table 3.

Table 3 Example of risk reducing process in ISS (Source: Bandyopadhyay et al. 1999, 441).

Type of risk	***Risk-reducing measures***
Natural disasters	Disaster recovery plan (DRP)
Data security risks	Backup files Password control Access codes Fingerprinting Palm printing Hand geometry Retinal screening Voice recognition Data encryption Call-back modems
Computer viruses	Monitoring computer usage Stringent audit procedures Employee education Use of company-provided software only Virus-scanning and virus-removing software
Strategic risks	Patent protection Innovative search for new ways to compete Formal planning and control procedures
Legal risks	Expert consultants to reduce legal risks

As we can identify from the table there is an absolute necessity for CIOs and CFOs and other senior managers to address these risks in all the levels of the organisation and

insuring that the reliability of data is not compromised by data security risks or other type of risk demonstrated in the table. As shown in table 3, the only clear mitigation strategy for natural disaster is a DRP, and the other risks are data, IT, strategic and legal ones that have the other measures like monitoring, backups, encryption, auditing, virus scanning and other mentioned procedures that fall under the umbrella of BCM as mentioned by Smith & Jamieson (2006, 25).

There is a need to get a clearer picture on disaster recovery for the students' perspective as well, since there has been limited research in the field recently and the exploration of the topic should be promoted throughout the IT industry. The trend has been for companies to rely less on mainframe technology for which disaster recovery was first formulated and shift through to the emerging distributed systems and LANs (Local Area Networks), WANs (Wide Area Networks) and other localised IT infrastructure for communication and data handling. Moreover, companies are utilizing more and more databases and computers, possibly in a distributed and dispersed location which has led it to become an increasingly client/server based network. Due to this shift, the disaster recovery plan has had to go a change to maintain these new technologies and infrastructure in companies rather than one mainframe in the early days (Hawkins et al. 2000, 223).

A US study in 1991 by the GAO (general accounting office) demonstrated that the levels of systems and data security controls in six major stock markets, namely, The American Stock Exchange, National Association of Security Dealers, The NYSE, The Midwest Stock Exchange, The Pacific Stock Exchange and the Philadelphia Stock Exchange which the following results in that 5/6 were diagnosed with weaknesses in system data security, 4/6 did not have a documented DRP and 3/6 did not have a backup computer ability. GAO advised improvements and the companies had to oblige since today, courts are beginning to hold organisations liable for inadequate or lack of a DRP (Xiao, Tate, Brown, Bussey & Richardson 1999, 115).

Although organisations are aware of the necessity of the continuity management plans, there seems to be a lack of preparedness across many industries when it comes to protecting the asset, be it data or other kind as is evident in the articles described by Xiao et al. (1999,115). This links us to the research sub-questions on DRP, "How is DRP managed in Finnish companies?", "What is the state of DRP in Finnish organisations?" and "What is the state of continuity planning and DRP in Finnish companies?", as the value of DRP to companies is addressed by these articles and in this way, the situation in Finnish companies can be studied further.

3.3 Organisational perspective on disaster recovery plan

In the eyes of the organisation, there is a need to look at the bigger picture when it comes to management of DRP and all its implications. It is clear that the resources, infrastructure, time and information required in handling and formulating the plan and organising the BCM system in accordance with the organisational requirement is just one part of the continuity management. Below is an illustration of the plans used in crisis in relation to the organisation. DRP (Disaster Recovery Plan), ERP (Emergency Response plan), CMP (Crisis Management Plan), Test plans and Media plans (Sheth et al. 2008, 224).

The aforementioned plans are based on the building blocks in the organisation that forms the core of the BCM system. These are 'strategy', which are the wants and needs of the customer, the risk tolerance level, and the valued critical processes of the business. Secondly, the 'plans' just mentioned as being the crisis communication plan, the emergency response plan and the disaster recovery and business resumption. Thirdly, the 'people', this comprises the skill set available, the trainability of the in-house personnel and issues like backups. Fourth block is the 'procedures', which comprise of everything that needs to be completed in order to perform a recovery. Finally, the fifth building block is the 'Technology', which involves all the IS and infrastructure that mediates the recovery (Sheth et al. 2008, 223-224).

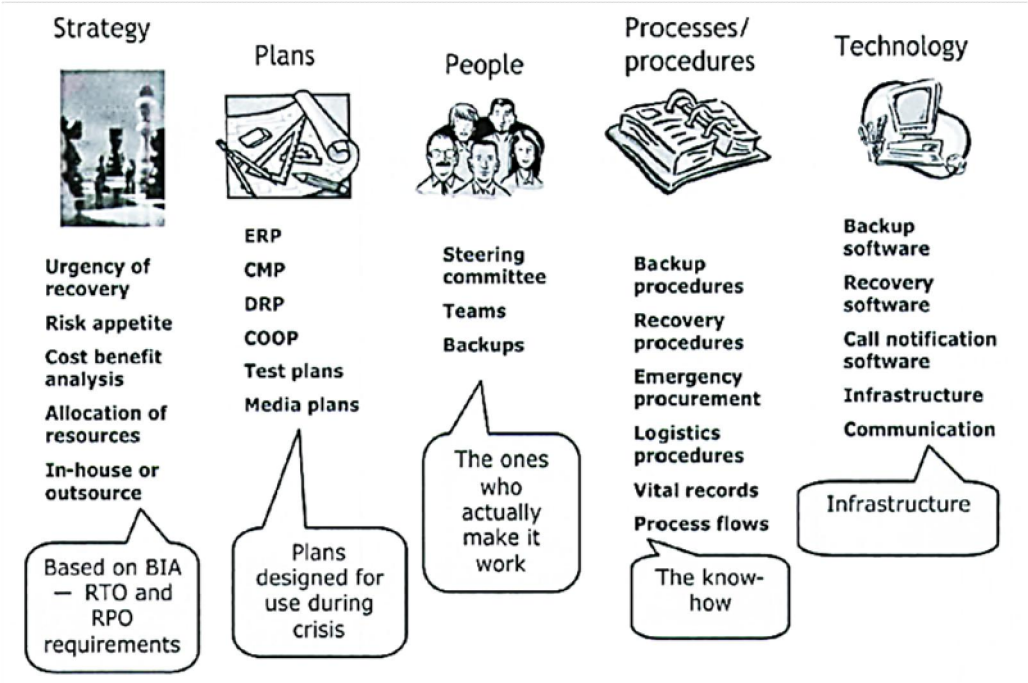

Figure 6 Organisation building blocks of BCM (Source: Sheth et al. 2008, 224).

Comparing to figure 1 (Nollau 2009, 53) it is found that these building blocks comprise a single organisation whereas figure 1 gave us a generalisation of the typical organisation with the core BCM in place. Furthermore, it is a mesh of the strategy, the plans, employees, processes and IT at the organisation that is intertwined in this DRP so that all these are safeguarded in case of a disaster. As seen in the figure 7, it is vital to address the ecosystem that the single organisation lives and breathes in with less restricted boundaries. Hence it is vital to understand that in the organisation of today, departments make use of ERMS (Enterprise Resource Management Systems), CRMS (Customer Relationship Management System), supply chain management system and their relationships with other organisations which in turn are supported by IS. It does depend on the type of the organisation whether the IS audit and DR team is internal or external, i.e. outsourced. For the typical organisation, the following BCMS can provide the extended view in relation to its off-site backup systems or storage, the alliance partners and other vendors that are related through the supply chain management (SCM), the alliance partners can have shared IT resources and processes, the customers, external agencies, government and also first action responders as shown in the diagram below (Sheth et al. 2008, 225).

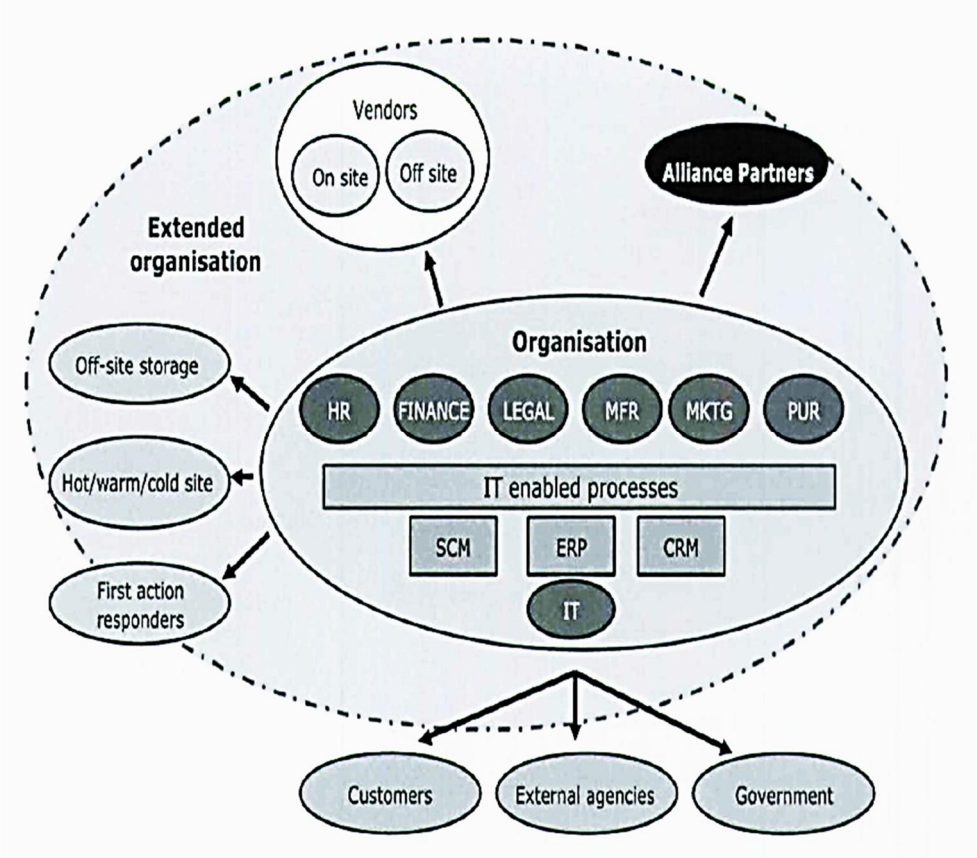

Figure 7 The Extended organisation with IT recovery processes (Source: Sheth et al. 2009, 226).

Figure 7 gives a picture of an organisation and its connections and alliances suppliers, vendors and outsourcing operations and this is quite important to understand since this extended organisation helps in the complete disaster recovery as explained earlier in the CISA review manual (2007, 457) which enables us to link to the value created for organisations by the DRP with the research questions

A study conducted by Ivancevich, Hermanson and Smith (1998, 31) where a 100 public listed companies were researched to analyse their relationship to the strength of the DRP and its effectiveness gave evidence, that indeed the size of a company is directly proportional to the overall effectiveness and advancement of contingency plan. It should be noted that this is not synonymous with the success of the company but the recovery from disaster and its effectiveness. Moreover, there was a positive correlation between the managements support for a given DRP and the strength of the DRP.

According to Xiao et al. (1999, 113), whether the disaster is natural, man-made, environmental or technological, organisations today are required to be socially responsible in the aftermath of disastrous situations. The organisation should be concerned with the focus or refocus on the bottom-line, which entails staff, loyal customers and the surrounding community. Hurricane Andrew destroyed the Miami-based Burger King and they had to relocate to a new area. The owner was concerned with getting the employees back on their feet so mental health after the trauma was the priority and he mentioned that to get Burger King back up and running the staff had to get back up on its feet first. A disaster recovery contract should exist if the company needs to have a sound BCM program and cannot utilise the in-house capabilities. The contract can range from a mid-scale recovery procedure to large scale (hot-site, cold-site or warm-site) relocation depending on the depth and necessity of the company, not to mention the budget and top management commitment as discussed earlier. The contract should be clear and state all the access and potential capabilities in case of a disaster and the company should test all these solutions beforehand.

Organisations have to consider the technical or socio-technical aspect of continuity management approach to recovery as well and this plays a vital role for DRP, BCM and BC in the strategy for the organisation which was also the case with the ISsec aspect discussed earlier by Anderson & Agrawal (2010, 616). Considering the topology of the approaches to continuity in an organisation, it is vital to understand the scope as depicted in figure 8. DRP is dealing purely with the technical and IT aspect of recovery. BCP and BCM are responsible for managing cross-functional and socio-technical aspects as shown in figure 9. Socio-technical approach of the activity stems from the combination of staff with IT issues and the cross-functional orientation means the range of the functions it covers in organisations. Recognising all the themes in organisational functionality and role of BCM in the figures 6, 7 and 8, the topology of continuity approaches identifies these in the simplest of manner within the realms of an

organisation (Herbane et al. 2004, 439).

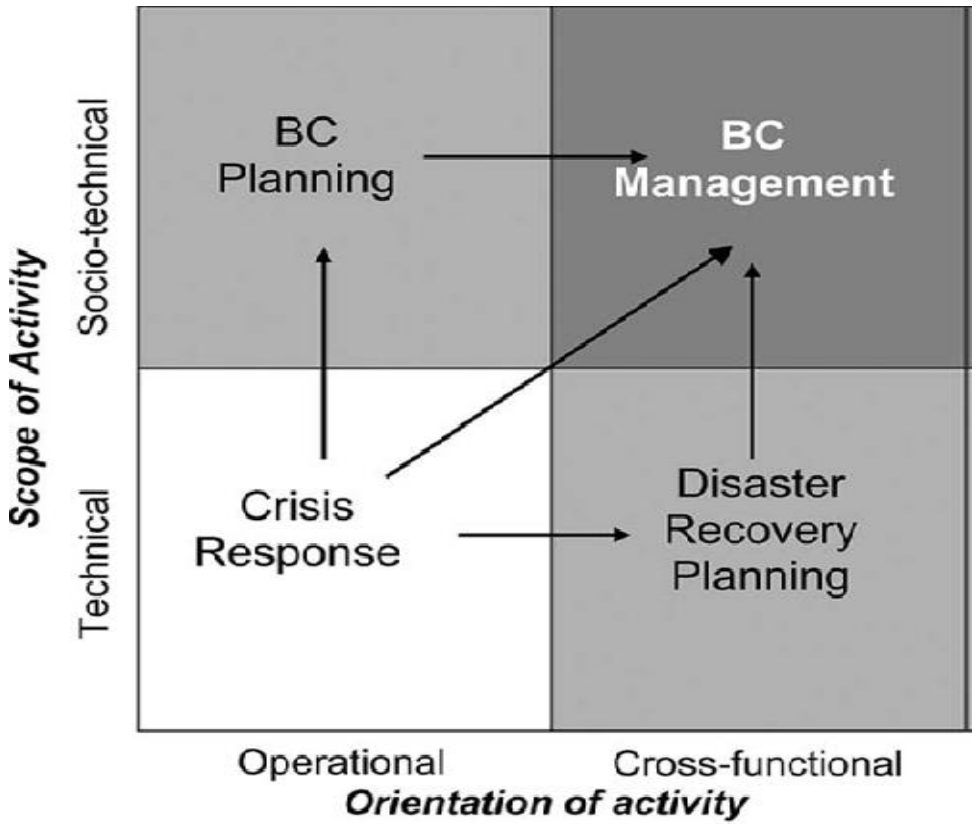

Figure 8 Typology of continuity planning approaches (Source: Herbane, Elliott & Swartz, 2004, 439).

Figure 8 also serves the purpose of categorizing the exact relation of BC plan, DRP and BCM which is vital to understand these concepts. Furthermore, this demonstrates the value of DRP (IT/technical) and the weight it carries in organisations, integrated into the BC plan and the entire scope of the BCM system, aligned with the ISsec functions and mitigation of IT risks as indicated by the arrows and the colour patterns, BCM, the umbrella management function being the darkest and the BCP and DRP being the lighter grey (Herbane et al. 2004, 439). Figure 7 illustrates the integration of the DRP with the other sections and levels in the organisation (in the form of building blocks) and this serves to complete the framework of the recovery plan within the company and the level of continuity it can achieve (Sheth et al. 2008, 224).

Coming along a quantitative study on the critical success factors of DRP by Chow and Ha (2009, 268) questions 129 managers regarding the implementation of DRP in information system functions. It indicates that there have not been enough quantitative study on this topic and provide the basis for ten DRP critical success factors on

organisational level and on a departmental level. They identify sixty-two information system function measurements which are utilised to formulate the ten critical success factors of DRP.

Developing an understanding of the kind of companies that strive to attain an effective and efficient DRP might be the beginning of a new era in information system security in any country (Ivancevich et al. 1998, 31). This is line with the understanding of the thesis author as well and will therefore gather information for this very purpose and show the value and importance of a DRP plan to be integral to the ISsec procedures and operations, as the rich literature that has been synthesised has revealed, is the key for truly understanding the value of DRP. These examples and illustration point out the links to the research questions and describe the importance of a BCM and DRP for organisations. In that manner, it will be quite interesting to understand the situation with DRP and BCM as a whole in Finland.

3.4 Formulation of a framework for the continuity plans

The organisational perspective on DRP and BCM shown in the above examples provides sufficient literature to conduct a research in Finland but before moving to the research methodology and data collection there is a need to complete and extract a framework for the plans. Most of the figures used in the literature indicate some aspect of the BCM and DRP within the organisation or on its own, and the following figure, figure 9 will try to reflect and build on those ideas and adapt a diagram which shows the plans with inputs and what needs to be done after that as well. Reflecting on the advent of disaster recovery and continuity plans from the different literature discussed in the theory by Sheth et al (2008, 225), the CISA review manual (2007, 447) and D'Amico (2007, 215) to name a few, it is found that there are certain traits that are repeating in these plans. The response phase that deals with the situation right after disaster; recovery phase, which is focusing on IT/IS infrastructure; resumption phase that focuses on business units processes depending on IT (containing the specific DR and CP); and finally the restoration phase or rebuilding phase dealing with normalcy of operations after the disaster of different proportions (Sheth et al. 2008, 225).

Hence, we arise to a situation where we can strongly reflect on these phases and consider them the driving force in the formulation of a framework for the purpose of this research, the 4R's framework, which is an amalgamation of the articles mentioned above indicating the phases of the continuity management. Figure 9 is a simple illustration of these plans in a phase format reflecting a timeline and having inputs from the BIA and covering the five blocks in an organisation as depicted earlier in figure 7. The step down approach is shown as this is a phase-wise process also mentioned by

D'Amico (2007, 215). The plans are organisation-wide and should be tested and updated regularly as well as shown in figure 9.

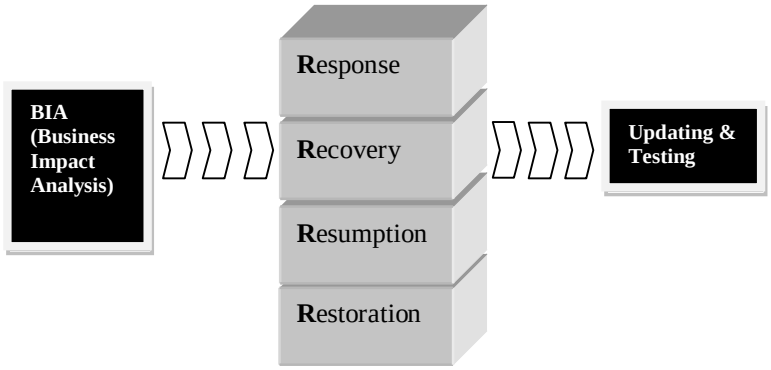

Figure 9 The 4R framework and phases of continuity planning (Adapted from CISA review manual 2007, 447; D'Amico 2007, 215; Sheth et al. 2008, 225)

The completion of the literature on BCM and DRP results in a link to the research questions again, the techniques, the value, the complexity and necessity of BCM and DRP has been found through the literature and the questions now need to be answered through a stringent research methodology and see whether or not this 4R framework is existing and aiding organisations.

4 RESEARCH METHODOLOGY

The research methodology brings in the knowledge from the literature review discussed regarding BCM and DRP and the finally incorporate that into what was found to be the underlying pattern in the 4R framework. This chapter focuses on the research design, data collection methods, selection criteria and finally the analysis of these data paving the way for next chapter which brings in the results.

4.1 Research design

The overall plan to connect the concept of the research problem, 'Weighing value the of continuity management: analyses of DRP in organisations,' with a useful and viable research methodology was very important for the cohesion and validity of this entire research (Ghauri & Grønhaug, 2002, 47-61). According to Ghauri and Grønhaug (2002, 171), case study research is an explanation of a management problem or situation, a question to be answered such as 'how' and 'why' and since the research question was trying to find out what is the value of continuity management and DRP in Finnish companies, it was the obvious choice for research methodology and the interviewing method of data collection was chosen after consultation with the supervisor.

Methodology of research was a case study of current BCM/DRP situation within organizations, and the situation was examined by interviewing representatives from 10 organisations and hence, formulating sound theme-based questions for the interviews was the best method to gather relevant and accurate qualitative data for analysis. Interviews were held in the companies and specific questions answered by the designated personal involved in those situations within their respective companies.

No data was revealed that could be linked to a single company and the results will be published in scientific journals and the master's theses which are going to be publicly available. For this reason, the company's sector and the simple details were revealed such as the position of the interviewee and the number of employees or the sector of industry they are belonging to.

4.2 Data collection and qualitative approach

The reason for qualitative method of interviewing was chosen because of the nature of the research problem, we needed to find what kind of value this concept of DRP and continuity management held and thus to get the holistic view, this mode was relied upon in this explorative research method.

The three major components of the qualitative research were as follows (Ghauri & Grønhaug, 2002, 87):

- Data collection; which was collected here in the form of structured and semi-structured interviews,
- Interpretative and analytical procedure; the techniques used to analyse these interviews, coding etc. to come at certain findings and
- finally the reporting of these in the form of theses.

Hence, thematic interviews of about 45 minutes to 1 hour were utilised. The questions were formulated on two levels, the technical and ISsec metrics of DRP and the organisational and strategic level (appendix 7.1.2). The research was a case study of medium to large Finnish companies, and the interviewees were in varying positions from top management to middle management. The interview questions themselves were chosen after collaboration with the supervisor and a colleague after being derived mostly from the literature and theory in the literature review. There were e-mails sent to medium and large Finnish companies from the different sectors and once again after input from the supervisor, the companies that replied were contacted back to see if they would agree to solicit an interview. A cover letter and the list of questions were sent to them at that point. The cover letter was used in correspondence with the university template supervised by another professor from the university in collaboration with the supervisor. Furthermore, the industry was different as well since a mix of industry was chosen from Finland to hopefully identify and show the varying concepts of DRP and continuity management.

The questions asked were simple and syntheses of the interview questions as to why these particular ones were asked are explained as follows:

- Size:

This was a straightforward theme since there was a need to reassure that company size is medium to large so the criterion for the sample is accurate.

- Human resource and responsibilities:

With the HR and responsibilities theme, it was inquired about what kind of people were involved in BCM, the responsibilities, implementation, whether they had a team for disruptions, with what kind of expertise and how many persons are involved with BCM and DRP..

- Communication and Embeddedness:

This set of questions underlined the communication and embeddedness theme of BCM and DRP and it attempted to inquire about communication and the manner in

which these plans and topics were discussed, implemented and followed in the interviewed companies. There were questions asking whether there was a strategic and precise role of reporting of ISsec issues with regard to continuity management. This was vital since this could shed light on the organisational structure and the top management, especially whether the interviewed CIO, CISO, CEO and ISM was solely responsible or was there a further business manager or board member in the company. Then, finally, we inquired as per the embeddedness of these plans and policies in the particular organisation, to see whether all employees follow them and were consciously involved and committed to these ISsec issues.

- Business continuity planning and processes:

As the theme about BCP and processes suggested, it was important to ask 'how' since we needed a more elaborate answer to the manner and ways in which top management supported and took part in DRP and BCP. We could have gotten an answer that simply stated whether the top management is involved or not, but this would not have be enough. Moreover, the manner in which the critical functions were prioritized was very important as well. This shed light on the critical processes, both business and IT based that needed to be assessed and this showed whether there had been some kind of risk analysis conducted at the company in question.

Then, we found out the schematics of IT infrastructure at the company which was also critical to understand how BCM and DRP were being managed, internally, externally or a mixture of both. Then we found out about the measures or examples of situations or existence of contracts and so on, security measures that had been taken by companies in dealing with suppliers, vendors and other customers when doing business, this shed light on the organisational environment and niche that the company existed in.

Then, we inquired about specific information security issues when the organisations contacted external companies or clients and vice versa. This was extremely important as it identified any specific measures to ensure security in the companies, network level, departmental level and organisational level. The situation about the usage of SaaS and security issues that needed to be handled in that regard was found out followed by the most important processes or functions in the company that without them, they would have failed more or less. Finally, this theme closed out with the inquiry about the business impact analysis and how this had an impact on the BCM and DRP.

- Attitudes and ownership:

Then there was the theme of attitude to BCM in the organisation which yielded information about any personal motivation to carry out DRP and BCP, in terms of

monetary grants perhaps from government, or even the industry and so forth. It was important to find out about the role of ISsec in the organisation and whether it was involved or not.

- Disruptions:

The disruption theme got into details about the kind of disruptions and disasters faced by the companies. This line of questioning was very important as we got a clear picture of the recovery, response, resolve and resumption procedures and measures that the company had taken to protect itself from different kinds of disruptions. This came into alignment with the 4R framework of DRP that the thesis researcher had formulated and would then use to identify the platform and critical success factors of good continuity management.

Then, it was inquired whether or not the company even had a BCP or DRP and also the role of ISsec was questioned which was very important as well since it showed how BCP, DRP were linked with ISsec in the organisation. Finally, the theme closes out with the inquiry about the vulnerability of any data the organisation might have faced in case of a disruption. It was important to understand this since different organisations would have valued different data and have dissimilar levels of vulnerability with respect to continuity management.

- Configuration and metrics:

The configuration and metrics theme started with management of the DRP in the organisation at hand and this gave us a concise picture of DRP, how it was handled and so on. In relation to this, it was also found out whether the company was capable of handling the disaster on its own. This showed the complexity of DRP and the extent to which it worked and gave the organisation the capability to handle it, major or minor in context. Then it was found out whether a third vendor or supplier existed that was responsible solely for these extreme scenarios.

It is investigated whether there are any specific measures of backups and redundant data security measures and how are they managed and discussed in DRP. Then we inquired about the recovery time objective and the recovery period objective with regard to the critical processes and functions in the company. This was very important as we understood the metrics of the DRP in the company. This emphasized the importance of the alternate process and whether it was enough to compensate for the main functions during the disaster. Then, finally in this configuration and metrics theme, the components of the plan itself, whether there were any phases, steps or procedures that were used to create a DRP were inquired about. These again led to the response,

recovery, restoration and resumption phases outlined in this DRP and gave a foundation of the 4R framework of disaster recovery that the thesis author had shown in the literature review in section 3.4. This was subdivided into two parts inquiring about the updating and testing of these plans in the organisation and this was crucial to identify those organisations that cared about continuity management.

- Legislation and standards:

The next line of questions inquired about the legislation and compliance with standards of security and BC, the ISO standards and the BC standards or even industry specific standards. This theme was based on whether the company had any incentive to follow these plans or did it simply to stay in the game due to strict regulations. It also gave us an idea of the understanding and involvement of top management in BC and whether these plans and procedures had a broader scope in the organisation.

- Strategy

The final theme dealt with the strategic view of BCM and DR on the organisational level. This theme inquired whether BCM and DRP gave any edge to the company in terms of the competition or just ensured the safety of the business, or enabled the business to exist and no more. This was very important since it described the true value of BCM and DR in the organisation. Finally, we closed out with improvement in the company, any improvement due to this planning and security measures.

4.3 Selection criteria

Characteristics of the interviewed companies (all Finnish) has been described in the table below and this was done after sending an e-mail with the cover letter (appendix 7.1.1) and the interview questions (appendix 7.1.2) as attachments to these companies. Out of all the companies, only one Finnish company did not wish to solicit an interview as it was not comfortable with giving out any crucial information regarding continuity management and disaster recovery.

It has been indicated in table 4 clearly that the companies interviewed were medium and large organisations and the interviewed personnel were of at least middle level management. Furthermore, the sector to which they belonged has been indicated which varied between insurance/banking, manufacturing and services to name a few. The respondents were termed as interviewee number such and such for confidentiality

purposes as per the agreed terms of this research method.

Table 4 Characteristics of the Finnish companies.

Interviewee #	***Industry/sector***	***No. of employees***	***Position***
Interviewee 1	Services	1100 (20% in administration and 40 in IT)	CISO
Interviewee 2	Insurance/Banking	1000	ITSM
Interviewee 3	Insurance/Banking	8000	CISO
Interviewee 4	Manufacturing	3000	ISM
Interviewee 5	Insurance/Banking	12,500	CIO
Interviewee 6	Manufacturing	250	SM
Interviewee 7	Insurance/Banking	36,500	HSF+RCO
Interviewee 8	Manufacturing/Services	110,000	CISO
Interviewee 9	Services	510	CIO
Interviewee 10	Services	700	ICTM

4.4 Data analysis

Coding was the method used for analysis of the interview transcriptions after consultation with the thesis supervisor. Since the research was of a qualitative nature, recognition was the first process of classifying and categorizing the transcriptions (Ghauri & Grønhaug, 2002, 123). From these transcriptions, concepts, themes, events, topical markers and synonyms were found with the aid of word analysis software, MS Word 2007. Coding was used to find the following (Rubin & Rubin, 2005):

- Concept: a word or term that represents an idea important for the research problem, for example an explanation of the idea of information security or organisational strategy.
- Themes: statements and explanations of what was going on, for example reasoning about motivations for security regulations compliance.
- An event: in our research was the occurrence of a disaster or disruption, other major change, testing etc.
- Topical markers were used for occurrences of names of other organisations, cities and places etc.

- Synonyms: were utilised to capture the essence of the language and meaning similar to the main concepts.

After identifying these five classification categories for the analysis, the actual data of the transcriptions was studied. Coding for events and topical markers was straightforward, but concepts and themes required more planning and insight. Hence, for this reason, the table below provided a schematic for this analysis.

Table 5 Analysis of data collection in interview method

Concepts	***Themes***	***Events***	***Topical markers***	***Synonyms***
Response Recovery Resumption Restoration Critical business function DRT/DRP/DR BCM/BCP/CM Functions Processes ISsec Availability BC standards ISsec standards Incident Response team IT Support Compliance	NDA SLA Redundancy and duplexing Mirroring Single point of failure BIA Risk management Risk mitigation Risk aversion VPN WAN IP telephony IS classification Mission critical (MC) Maturity level	Disaster Disruptions Updating Fires Natural disasters Testing	Number of employees Number of IT personnel Other numerical data Locations Cities Company names	Respond Normalcy Resume Recover Business units Restore Recognise Recognition Standards Legislation IT support personnel Comply Regulation

A colour code was defined to be able to mark this in the interview transcriptions, yellow for concepts, green for themes, grey for events and red for topical markers and turquoise for synonyms.

Validity was vital for the data analysis and this was shown in the accuracy of description, interpretation, theory formulization and generalization of qualitative data gathered. It was not enough to claim a valid set of results as depicted by Ghauri and Grønhaug (2002, 139) but the thesis author also tried to justify the actual findings by demonstrating that they existed in the companies studied at the very least. Reliability of the data was demonstrated as the analysis results or interpretations were discussed amongst, the thesis author, the supervisor and the colleague.

5 RESULTS

The results are discussed here according to the interview themes about the technicalities of DRP and then the relationship with the 4R framework, the research questions and the literature review is assessed and presented.

5.1 The 4 R's and information security

The critical issue was to investigate the current situation in continuity management, DRP and find out if they are of value to the companies. The objectives were to collect information through interviews (10 medium to large) of companies in Finland and identify whether the 4R framework exists.

Moreover, to identify the situation with BCM, BCP, DRP and ISsec and link the RQs and the findings and compare them and finally to identify what are the good practices and how embedded they are.

5.2 Response

Reverting to the material found in the literature review on response phase of the 4R framework, it was found to be the plan of actions right after a disaster or disruption and consisted of the emergency response plan and crisis communication plan. In the emergency response plan were the routine actions to safe guard personnel and staff in the vicinity of a disaster and in the crisis communication plan were the chain of communication about the disruption, internal or external, to the media and even to a national level (Sheth et al. 2008, 225; D'Amico 2007, 215).

Regarding the findings from the interviews on the response phase, all 10 companies interviewed had the basic response mechanisms or procedures in place, even if they did not have an intricate documented plan; they had some 'emergency response plan' present. Hence the first response plans of the 4R framework were present in all companies. Subsequently, the crisis communication plans were present in 9 of the 10 companies interviewed. The company in which the first response plan did not exist was smaller in size compared to the others. These plans were quite identical in the companies as the line of communication was followed in case of major disasters and CEOs and top management got involved along with outside vendors and partners, thus identifying internal and external communication and one interviewee also mentioned:

> *Each and every unit makes their own plan and then they also have to communicate in different ways. For example, if you think about our relationship manager, she has got totally different kind of attitude because she is handling the public relations and answering all the questions of journalists and so on. (IT service manager, Insurance and Banking company)*

Then, with regards to the crisis communication plans, another interviewee said:

> *In some way you have to communicate and report to some direction depending on what it impacts and what it doesn't. Usually we report to some direction so in that way the disruptions are handled so that we get them working as soon as possible. (Information and Communication Technology manager, Service company)*

Then with regard to emergency responses, one interviewee mentioned:

> *Yes, there is one, mostly business and production expertise. There has been some training to get all staff moved from a location to here in case of evacuation and how to continue operations on this location. There are IT personnel involved in these groups. (Chief Information Security Officer, Services company)*

It is evident from these respondents that the response phase of the 4R framework existed in these interviewed companies and is in alignment with the literature on the constituent plans, the emergency response plans and the crisis communication plans.

Regarding the BCM, BCP and specifically DRP, 3 companies did not have them in a documented form but did have risk aversion and ISsec policies and procedures with some recovery plan in place. Some of the 7 companies had strict BCP plans for every individual business unit complete with updating and testing on all levels, organisational and departmental. Of those companies, one interviewee mentioned:

> *We have both. And the rough idea is that BC is done by business and together with the system specialist in IM and then DRP is more of a technical thing and that is done by the service provider and we kind of oversee it and we make sure they have sufficient DR and I oversee that our DR actions regarding the systems that we support internally, the systems, and then the technical DR are in line and that everything should go smoothly. (Information Security Manager, Manufacturing company)*

These results revealed insight on the existence of the BCM in accordance with the priority and value it held in all organisations interviewed. The 4R framework existed in the larger Finnish companies and had top management support. In this way, it was found to be making organisations more resilient and assured in time of disaster as per the definition of BCM (BSI 2006). In the companies that lacked the resources for such plans, the size was the factor and also the sector it belonged to.

This links to a research question, sub-question 4. “What is the status of BCM in companies?” and now it can be answered in the way that it does exist in the interviewed companies as seen in throughout the interviews in the form of how Finnish companies respond to disaster and crisis situations. This leads us to support this phase as it does exist in companies and additionally in the literature as described.

5.3 Recovery

Now, coming to the second phase of the 4R framework, the recovery phase is focused on IT/IS and the workarounds or alternatives which consist of resource dependency plans and workaround plans. The resource dependency plans help the organisation identify the infrastructure needs. The work around plans allows the business to continue functioning from the point of disruption until the completion of recovery as mentioned by Sheth et al. (2008, 225) in the literature discussed earlier (chapter 2.2).

Regarding the findings from the interviews on the recovery phase, redundancy, duplexing, mirroring, data-centre solutions and backups were the procedures that took care of disaster handling in all the companies. Backups (tape backups, offsite, on-site) were the prime processes in those companies that were relatively smaller. Redundancy and mirroring processes were taking place in the larger companies. These were the work around plans and 9/10 companies interviewed had them. As one interviewee mentioned:

> *Well, for technical problems for example we have redundant networks. We have somewhat redundant data centres depending on the service or depending on the system, some parts are redundant and some are not but then we are getting the capacity service from the service provider so in some cases we have the option of moving from datacentre to another just moving the data from datacentre to another and getting the same service from another datacentre. Then, depending on system for technical failures, our systems mostly have 3 different environments. (Information Security Manager, Manufacturing company)*

Additionally,

> *It depends on the damage done, for example in the case of fire we have cooperation with another company in different locations and we can utilise each other's facilities if one is down. We do not compete with each other since they are concentrated elsewhere. (Chief Information Security Officer, Services company)*

The company that did not have an adequate workaround was one of the smaller companies interviewed in terms of organisation size. These examples of workarounds or alternative plans that are started in case of disaster until the recovery is completed in the companies interviewed indicate the presence of workaround plans, a significant constituent of the recovery phase of the 4R framework. 7 companies had some kind of resource dependency analysis and some ISS classification done with regard to applications or systems, personnel, equipment, vendors and their internal and external dependencies, one interviewee mentioned:

> *...Resilient meeting systems (Corporate business continuity forums), business management (BM, IT and business), mission business task critical (MBTC), prioritization and dependency management of processes and function exists in the organisation. . (Chief Information Security Officer, Manufacturing and Services company)*

A second example of resource dependency:

> *It comes from the Risk management board and they do some kind of risk analysis and the information system classification comes from the main directors. They decide what are the most critical business needs and BIA so the board of directors and the risk management team decides on these as they own the budget. (IT Service Manager, Insurance and Banking company)*

Three companies that did not have an adequate measure of resource dependency analysis did have some form of contracts to insure their assets. And to quote one of those interviewees:

> *Well, in some areas yes, we have some critical parts so that we have partner and expert partners with which we have built those and help is*

> *available from them if necessary and we have used the help because of the capacity. But these are only for very critical purposes so mainly related to data or firewalls or branch fusions. (Information Communication Technology Manager, Services company)*

Comparing these findings to the literature on recovery phase of the 4R framework, we can deduce that there is indeed such a phase as argued above consisting of the workaround plans and the resource dependency analysis. The best practices were examined by interviewing the companies and the information revealed that redundancy, mirroring and duplexing brought about the greatest results in recovery from disaster. In larger Finnish companies, this was the policy and the BIA was the input for the all the continuity plans along with some critical process operations identification function. The plans were in phases which were identified from the literature to be the 4R framework. This BCP was tested and updated yearly or biannually in these organisations.

Moreover, the researches sub-question number 3, "What is the best practice in companies when it comes to dealing with continuity management and disaster recovery?" can be addressed with this analysis of the recovery phase as we see the state-of-the-art redundancy and mirroring in quite a few companies together with complete resource dependency analysis. Thus we can support these findings as they are complemented with the literature on the plans.

5.4 Resumption

Reiterating from the previous literature review on resumption phase, it consists of the disaster recovery plans and the continuity of operations plans or business resumption plan. The DRP contains the IT recovery processes and critical business functions and business resumption procedures. The DRP was discussed in detail in the literature and it was evident that after BIA (Business Impact Analysis) and critical operations are identified; the disaster recovery plan is formulated based on RPO (Recovery Point Objective) and RTO (Recovery Time Objective). These RPO and RTO aid in identifying the recovery strategies to be used in the DRP. Therefore, to come to that phase where disaster tolerance for certain processes can be accepted gives a clear understanding of the procedure with respect to time (Sheth et al. 2008, 225; D'Amico 2007, 215; CISA review manual 2007, 449).

Regarding the interview findings on DRP and business resumption of the resumption phase, all the companies interviewed had at least one if not more critical business functions. Only 1 of them did not have any prioritisation done. The critical functions in that company were known but the interviewee did not know how the prioritisation had

been done. This was the company with a smaller number of employees compared to the other larger companies that had critical process prioritised and documented. 1 of those 9 did not have documented prioritisation and the interviewee mentioned:

> *These two functions are prioritized although there is no formal documentation as such and the people working in these situations are there for 45 years so they really know the systems in and out. Although it is changing now since these people are nearing retirement and the tacit knowledge is there and it is a real issue when new people start jobs and this has to be documented and it is quite critical. (Chief Information Security Officer, Services company)*

Another interviewee stated:

> *We have a list of functions. We have some priorities from legislation for instance which come first of course, those we have to take care of and then we have a list of other functions which come after those so it is done. (Chief Information Security Officer, Insurance and banking company)*

The inputs in 7 companies for the DRP came from BIA and some prioritisation of business as mentioned and one interviewee claimed:

> *Template is based on BIA in that sense that understand what are the main processes and the most important processes in each unit. And based on that create the plan. So it is. (Risk Compliance Officer, Insurance and Banking company)*

The recovery point objective and time objective were quite different in different companies as they were having different critical business processes. One interviewee mentioned:

> *Well it depends on the disruption. For the critical components we have a 4hr time objective. Those that are dependent on the supplier those that are related to some HW time objective or connection time objectives. That means that the recovery procedures are started within 4 hours so it depends on the disruption. (Information Communication Technology Manager, Services company)*

And to include a comment on the business resumption which is the re-opening of the business operations after a disaster:

> *Yes, that is actually how it goes that all these plans are made so that there is for example for us we know what has happened then we have a plan, we make decisions on what to do and so on, and then how to come back to the normal life and I think that is the most difficult part of it, returning to normal. (IT Service Manager, Insurance and business company)*

The disaster recovery was described as being a plan for recovering IT and IS assets in an organisation in the time of a disaster or disruption and was understood as being a plan among other plans in the BCP, which in turn was under the umbrella of BCM. Then it was identified as being based on the RTO, RPO, which in turn were formulated after a critical process analysis and business impact analysis from the literature.

The case in point in large companies that contained more than a 1000 or so employees, the DRP was documented and managed according to either compliance with legislation (not certification) and 'cherry-picking' the best parts to use from the standards like ISO27001, ITIL and BC25999. Only two companies followed a framework, COBIT and ITIL as found out from the interviews and the management of DRP was tested and updated and had support from top management in these companies and it was also found that some were proactive and not reactive. The existence of the DRP should assure against disruptions and the BIA, RTO and RPO are resource intensive processes that require time and money. Prioritisation of critical processes was the key to formulating an adequate disaster recovery plan and again, 3 of the companies interviewed were found to lack distinct documented DRP or BCP.

The focus of companies was varying due to the diversity in the sectors, and the critical operations were different in companies so the management of assets was also dissimilar. Finally, disaster recovery was identified to be conducted, formulated, tested, updated and supported and managed in the companies that required and perceived it as important to their resiliency to disruptions, major or minor. After examining the contents of the plan and how it is managed and formulated in companies, it was discovered that the support from top and senior management varied and the communication of the plan varied in companies. Some companies made sure every employee adhered to the process and acknowledged them by having some form of monitoring or models specifically designed to motivate and escalate the awareness of the plan amongst the staff.

The 3 companies that lack sufficient documented plans had ISsec policies in place and sufficient teams to manage disruptions. Otherwise they had SLAs and NDAs that

made sure the assets and critical processes were insured. The existence of the plans in detail in the bigger companies made it evident that DRP and continuity management were organisation-wide plans covering all IT and services. Finally, the status of the plans was discovered as being of different value to different companies, with regard to the sector and size of the organisation respectively. DRP should be given more weight in companies and not just ignored or done after something happens, since that was the implication from most interviews.

We can reflect from these findings that this is in agreement with the literature review on the DRP plans and the resumption phase and thus we support the literature on DRP and resumption phase of the 4R framework. The link to the research sub-questions 1 and 2, "How is disaster recovery managed in companies?" and "What is the state of disaster recovery planning in companies?" is found in this phase as we have shown how some Finnish companies manage DRP and what is the status with the interview findings and literature.

5.5 Restoration

Restoration phase of the 4R framework of BCP according to the literature consists of the normalcy after the event of a disaster and that included the business restoration plan. This plan dealt with the salvage and recovery of the site (if needed) and returning to normalcy of the processes and operations of the organisation (Sheth et al. 2008, 225; D'Amico 2007, 215).

Regarding the restoration phase, the interviewed companies had some normalcy plans as they were considered the most important part of the plans (return to normalcy of operations after the disaster was considered the most crucial). One interviewee mentioned:

> *Yes, that is actually how it goes that all these plans are made so that there is for example for us we know what has happened then we have a plan, we make decisions on what to do and so on, and then how to come back to the normal life and I think that is the most difficult part of it, returning to normal. (IT Service Manager, Insurance and business company)*

Another example on normalcy of operations:

> *Every factory has its own BCP and there is no separate handling as the plans are aligned and BCP consists of the following: Response, Recovery, Resumption and restoration. (Chief Information Security*

Officer, Manufacturing and services company)

On the other hand, one of the companies did not have the restore plans as they did not have the resources to cope and salvage from a disaster according to one interviewee:

> *Never, not in any case. Our manufacturing is very equipment dependent. There are big investments and big machines that we can't really duplicate in any case. (System manager, Manufacturing company)*

Another interviewee stated regarding the value of CM:

> *At some point senior management might question some of the investments that are connected to CM but they have always gone through because they have gained value. (Chief Information Technology Supervisor, Insurance and banking company)*

Additionally:

> *First we need to identify what are the parts, what does it consists and what is the weight of these listed parts, and how continuity of these systems is sufficient. It requires documentation and it is very important when conducting business impact analysis as it connects business needs and IT recovery and ISsec. (Chief Information Security Officer, Services company)*

From the above examples on the presence of a restoration plan we can revert to the literature regarding the plan as well and comparing it to the findings in the interviewed companies, it is seen that it existed in those companies that have conducted a BIA, and have a tested and updated BCP.

There is a link to the main research question, "*"What is the importance of continuity management planning in companies?"* as we can finally acknowledge the importance of a BCP and conclude that it is indeed composed of the 4R framework as shown in these analysis of interviews and the previous literature together with its significance in a company that uses it to handle disruption. The importance is discovered to be two fold in many companies; it is 'business and IT/IS linking' and 'value-gaining' as well. So these findings can now be justified as being in harmony with literature review on the 4R framework thus leading us to support the framework, empirically and through literature as well.

5.6 Information security

Information security was discussed in the literature review and adjudged to constitute the CIA model, the confidentiality, integrity and availability of crucial information and assets to a company, and after some arguments, placed alongside the recovery plans under the BCP. Moreover, with respect to BCP, ISsec was the availability feature of the information (Botha & Von Solms 2004, 329; Smith & Jamieson 2006, 25).

In the interviews, the role of ISsec was quite different in most companies as some had very clear policies and some had more vague ISsec policies and were not clear on the CIA model. Even then, ISsec was considered vital in all organisations questioned and was present in one form or the other. There was confusion though to exactly where it could be placed, (as in the literature, it is placed under BCP together with the DRP), one interviewee said of the role of ISsec:

> *So, that is one linkage between ISsec and DR but of course there are security issues and they are properly handled and they have to be properly handled. It could be someone else doing the DR things so it's kind of, ISsec is a bit hard to place, it's somewhat hard to place anywhere. Overall, it should cover everything more or less. (Information Security manager, Manufacturing company)*

A second mentioned:

> *Data security was handled case by case and this included corporate financial data, data protection, and the confidentiality, integrity and availability model of ISsec. (Chief Information Security Officer, Manufacturing and services company)*

Regarding the availability feature that links BCM and BCP to ISsec, an interviewee mentioned:

> *It is a question of availability. Due to working specifically in the IT department, the view of the business people cannot be given but since communicating directly with the business people, we would say availability is the essence of continuity management. (Chief Information Systems Officer, Services company)*

We cannot be certain and answer where to place ISsec from these findings but there is the link between ISsec being the availability feature of BCP (Botha & Von Solms 2004, 329) and found out that in some companies interviewed, that was indeed the case.

Moreover, the CIA model of ISsec was mentioned in these interviews thus the findings on ISsec are partially supported as the availability aspect and the CIA model were found in the companies interviewed but the ISsec policy was considered an organisation wide policy and not existing according to the literature review, under the BCP (Smith & Jamieson (2006, 25).

The link to the research question comes indirectly here, as it incorporates some part of the main question, '*What is the importance of continuity management planning in companies?*' It was made clear in the literature that ISsec was part of BCP which also contained the plans and specifically DRP. Hence it can be concluded that ISsec is indeed a part of continuity management as also seen from the availability aspect of business continuity from these companies, and BCM cannot be complete without it.

6 CONCLUSIONS AND DISCUSSION

6.1 Conclusions

The main objective of this research was to analyse the current situation in Finnish medium and large companies regarding continuity management. Hence it was an attempt to answer the main research problem by interviewing and examining the situation in the companies, '*What is the importance of continuity management planning in companies?'* This problem was divided into sub-questions to better explain and identify the concept of continuity management and its constituents and to recall from the research questions:

- How is disaster recovery managed in companies?
- What is the state of disaster recovery planning in companies?
- What is the best practice in companies when it comes to dealing with continuity management and disaster recovery?
- What is the status of BCM in companies?

First of all, disaster recovery and disaster recovery planning was identified in the interviewed companies. The large companies that contained more than 1000 or so employees, the DRP was documented and managed according to either compliance with government policies or using the best parts from standards like ISO27001, ITIL and BC25999, or both. Only two companies followed a framework, COBIT and ITIL and the management of DRP was tested and updated and had support from top management and it was also found that some were proactive and not reactive. Critical process prioritisation was the key to formulating a disaster recovery plan and three of the companies interviewed were found to lack distinct documented DRP or BCP. Hence the management of the plans was different and the interviewed companies that incorporated BCM and BIA understood the 4R framework; utilised the BCP and valued it since prioritisation assured some critical process identification and protected the organisation in time of disruption. So, these were some conclusions that could be drawn as to the manner in which the interviewed organisations managed DRP.

Secondly, the state of DRP was identified and found to be varying across the companies and sectors. Further examination indicated the formulation and all other related procedures that resulted in drafting the DRP. Top management support and communication of the plan was identified to be different in different companies. This could be due to the size of the organisation and the sector of the industry that it belonged to, and perhaps correlate between the number of employees and the

responsibility and commitment of the organisation to be ever ready in times of crisis and protect all assets. Three companies that were found to lack the specifically documented plans did have alternatives as mentioned in the empirical findings, either in the form of assurances and contracts such as NDA's and SLA's and these provided them with the sufficient security they needed. It can be argued that DRP was given more weight after something disruptive had occurred and only in a few companies, it was found to be a 'preemptive plan' of action. These were some conclusions that can be drawn from the researched companies and the question is answered to whether the DRP is in a good state in companies or not.

Thirdly, to reiterate from the findings regarding the recommendations or best practices the information revealed that redundancy, mirroring and duplexing brought about the greatest results in recovery from disaster. In larger companies, these were the policies and the BIA was the input for the all the continuity plans along with some critical process operations identification function. The plans were in phases which were identified from the literature to be the 4R framework. This BCP was tested and updated yearly or biannually in these organisations. In accordance with the findings smaller companies (less than 1000 employees comparatively) had assurances and backups to secure their data, but they were concerned more in terms of information security and concentrated on the CIA model when it came to protecting their assets. In that way, it could be argued that the best practices are really impossible to generalise even with such concrete plans and policies in place. These were some conclusions that could be made after assessing the best practices of companies in dealing with disasters and disruptions.

Finally, the question about the status of BCM was answered with the examination of the literature review and its comparison with the interview findings. The results revealed insight on the existence of the BCM in accordance with the priority and value it held in all organisations interviewed. The 4R framework existed in the larger Finnish companies and had top management support. In this way, it was found to be making organisations more resilient and assured in time of disaster as per the definition of BCM (BSI 2006). In the companies that lacked the resources for such plans, the size was the factor and also the sector it belonged to as found in the interviews. Moreover, ISsec was considered to be an important part of IT and the organisations interviewed recognised the importance of the CIA model and the availability aspect that was aligned with the BCP although it was not clear where exactly ISsec fit into the interviewed organisations; it was an integral part of the BCM. These were the conclusions on the state of BCM in the companies and it was identified that the smaller sized companies that were interrogated did recognise the importance of BCM even though they did not incorporate it in terms of ISsec.

BCM, BCP, DRP and ISsec are all part of the equation that needs to be balanced within an organisation. This is in accordance with the findings and literature as these are

aligned within the 4R framework together with the inputs, BIA and their testing and updating provide some added security for the organisation in return that it will indeed to survive a disaster. These questions and the main research question focus on the issue of BCM and the 4R framework aids organisations which is in accordance with the findings as analysis has indicated and also come in line with the opinion of the thesis author. The presence and necessity of BCM and DRP has been found in the interviewed companies and the questions have been answered through this research methodology indicating that the 4R framework exists and aids organisations; therefore it can be argued that it is of value to them.

6.2 Discussion

These sub-questions answer the main question that was segregated initially to explain the continuity management's constituents. ISsec (CIA model) exists in companies but needs to be clarified as to where it fits into the organisation in accordance with the thesis author's opinion. It can be recommended as it was in the literature as being part of the BCP and containing the availability aspect in the plans as was found to be the case in both, literature and case findings. There was ambiguity in the concept of ISsec as the analysis of the findings in ISsec indicated earlier and this research aimed to clarify some of that through the literature review (Botha & Von Solms 2004, 329).

The term disaster recovery was in some companies thought of as only dealing with natural disasters only as mentioned and the plan unfolded after the disaster had struck in view of the thesis author. Finally, what can be recommended are the best practices together with a firm critical process identification and prioritisation and of course that is achieved only after a BIA. This makes it possible for the company to understand what processes and functions are really required and be made available and accessible to staff and customer at all times, while maintaining integrity and confidentiality. It can be argued that there is a relation between the framework, the resources and size of the organisations as well; the bigger the number and size of the company, the better the continuity management and recovery plans.

Since the main problem of the research was to find out the value of holistic continuity management in companies, it can be argued that the existence and implementation of this function was discovered to be a significant advantage and interviewed companies view it as such. These 4Rs framework signifies the plans and the inputs that existed in the companies that utilised them to their advantage and had shown resiliency by maintaining their business operations!

6.3 Limitations

It is important to recognise and understand the restrictions in the research as they influence the work and the validity increases by acknowledging these limitations which were found in the thesis work since there was a strict timeline for the project. Moreover, the interviews consisted of only medium and large sized Finnish companies; hence the findings may not be applicable to different small sized-companies and enterprises. Limitations also existed in the sense that all the thesis literature could not be scholarly journals and articles and some of them had to be from technical journals since the topic was fairly current. There however, is some benefit as this technical journal represents the latest information on the topic being used in the field. Another limitation could be proposed that the number of interviewed companies was not enough to generalise the interview results. Moreover, a few companies were not interested to solicit an interview altogether due to competition and information sharing issues.

Furthermore, the disclosure of companies' names and the anonymity aspect taken into account (interview cover letter) proposed a limitation as the research could not directly name companies but only the sector, size and position of the interviewee. On the other hand, these companies agreed to grant and solicit interviews so this in turn helped the overall interview process and made the research possible. There could be some further testing and analysis with an increased timeline so the research could include a quantitative analysis to make it possible to generalise these results. Credibility, validity and integrity of the project work are enhanced by acknowledging these along the course of the research and taking some measures to minimise their affect and to take opportunity of the timeline perhaps.

7 REFERENCES

Anderson, C. - Agarwal, R. (2010) Practicing safe computing: A multimethod empirical examination of home computer user security behavioural intentions. *MIS Quarterly*, *34*(3), 613-A15.

Bandyopadhyay, Kakoli - Mykytyn, Peter P. - Mykytyn Kathleen (1999) A framework for integrated risk management in information technology. *Management Decision*, 37(5), 437-444.

Bhavani, Suresh (2010) Disaster--Is It a Blessing in Disguise and Is BCM the Boon? *COBIT Focus*, 2010(1), 5-7.

Botha, Jacques - Von Solms, Rossouw (2004) A cyclic approach to business continuity planning. *Information Management & Computer Security*, 12(4), 328-337.

Bradbury, C. (2008) Disaster! Creating and testing an effective Recovery Plan. *The British Journal of Administrative Management*, 14-16.

Cerullo, Virginia - Cerullo, Michael J. (2004) Business Continuity Planning: A Comprehensive Approach. *Information Systems Management*, 21(3), 70-78.

Chisholm, P. (2008) Disaster Recovery Planning Is Business-Critical. *CPA Journal*, 78(7), 11.

CISA Review Manual 2007 (*Certified Information Systems Auditor*) Chapter 6, Business Continuity and Disaster Recovery, pp. 441-478.

D'Amico, Vin (2007) Master the three phases of business continuity planning. *Business Strategy Series*, 8(3), 214-220.

Epich, R. - Persson, J. (1994) A fire drill for business, Information Strategy: *The Executive's Journal*, pp. 44-7.

Gallagher, M. (2003) Business continuity management. *Accountancy Ireland*, 35(4), 15-16.

Gallagher, M. (2007) Business Continuity Management: Emerging Standards. *Accountancy Ireland*, 39(3), 34-36.

Ghauri, Pervez - Kjell, Grønhaug (2nd ed.) (2002) *Research methods in business studies*. A practical guide. Financial Times, Prentice Hall

Gibb, F. – Buchanan, S. (2006) A framework for business continuity management. *International Journal of Information Management*, Vol. 26, 128-141. Retrieved from (http://www.sciencedirect.com/science/article/B6VB4-4JN2P51-1/2/57980f789e3c81f88a500981a33a3b45)

Google Scholar Search Site: Kristen Noakes-Fry (2008) Business Continuity and Disaster Recovery Planning and Management: Perspective, 1-15. <http://www.availability.com/resource/pdfs/DPRO-100862.pdf>, retrieved 1.3.2010

Hawkins, Steve M. - Yen, David C. - Chou, David C. (2000) Disaster recovery planning: A strategy for data security. *Information Management & Computer Security*, 8(5), 222-229.

Herbane, Brahim - Elliott, Dominic - Swartz, Ethne M (2002) Business Continuity Management. A Crisis Management Approach, Routledge, London and New York, 224 pp. (Book review)

Herbane, Brahim - Elliott, Dominic - Swartz, Ethne M (2004) Business Continuity Management: Time for a Strategic Role?, *Long Range Planning*, Volume 37, Issue 5, October 2004, Page 386, Retrieved from (http://www.sciencedirect.com/science/article/B6V6K-4DDXMGV-3/2/e1c4937ab2498ea71411e90d533776f2)

Ivancevich, D. - Hermanson, D. - Smith, L. (1998) The Association of Perceived Disaster Recovery Plan Strength with Organizational Characteristics. *Journal of Information Systems*, 12(1), 31-34.

Kotulic, A.G. – Clark, J.G. (2004) Why there aren't more information security research studies. *Information and Management*. 41 (5), pp. 597-607.

Krell, E. (2006) The Case for Business Continuity Management. (cover story). *Business Finance*, 12(4), 20-28.

Nollau, B. (2009) Disaster Recovery and Business Continuity. *Journal of GXP Compliance*, 13(3), 51-58.

Ross, J. - Weill, P. (2002) Six IT Decisions Your IT People Shouldn't Make. *Harvard Business Review*, 80(11), 84-92.

Rubin, Herbert - Rubin, Irene (2nd ed.) (2005) *Qualitative Interviewing: The art of hearing data*. Thousand Oaks, pp. 208-209, Cal. a.o.: Sage

Security log (2006). *Computerworld*, 40(26), 33.

Seow, K. (2009) Gaining senior executive commitment to business continuity: Motivators and reinforcers. *Journal of Business Continuity & Emergency Planning*, 3(3), 201-208.

Sheth, S. - McHugh, J. - Jones, F. (2008) A dashboard for measuring capability when designing, implementing and validating business continuity and disaster recovery projects. *Journal of Business Continuity & Emergency Planning*, 2(3), 221-239.

Smith, S. - Jamieson, R (2006) Determining key factors in E-government information systems security. *Information Systems Management*, 23(2), 23-32.

Toigo, John William (1989) *Disaster recovery planning: Managing risk and catastrophe in Information Systems*. Yourdon Press, Prentice Hall, NJ.

Wing S. Chow - Wai On Ha (2009) Determinants of the critical success factor of disaster recovery planning for information systems, *Information Management & Computer Security*, 17(3) ,248 -275.

Xiao, L. - Tate-Smith, L. - Brown, S. - Bussey, C. – Richardson Johnson, D. (1999) Disaster recovery planning: Methodology and implementations in regional organisations. Allied Academies International Conference. *Academy of Information and Management Sciences. Proceedings*, 3(1), 101-118.

8 APPENDICES

8.1 Interview cover letter

Interview request concerning Business Continuity Management and Disaster Recovery Planning

On behalf of the Turku School of Economics we solicit an interview session with your company, as part of the curriculum for the completion of the master's thesis (TJPG course). The aim is to provide IT students with a better understanding and skill-set in managing different types of critical situations in dealing with business disruptions.

The goal of the interview is to learn about your company's Information System Security issues and their value for Business Continuity Management and Disaster Recovery Plan to your company.

The interview themes are attached to the mail. However, the interviewee may bring up other relevant issues during the interview. The targeted interview duration is 45 minutes to one hour. We would appreciate if the interview language could be English, but we are also able to interview in Finnish.

The information will be used as a part of two master's theses in Turku School of Economics and also as a starting point for a larger survey focusing on Information Security in Finnish companies. We will be interviewing also other Finnish medium-sized and large companies on different sectors, and we will provide you a report based on analysis of the interviews. All the interview material is treated as confidential and we can guarantee nondisclosure of any business sensitive information.

We will be contacting you within [3] business days to discuss this project. If you have any further queries, please do not hesitate to contact us.

Thank you for your time and consideration.

Sincerely

Jonna Järvelainen	Danish Islam	Antti Lehtimäki
D.Sc. post-doctoral researcher	(Master's thesis researcher)	(Master's thesis researcher)

8.2 Interview questions with companies

I Human resource and responsibilities

a) Who is responsible for BCM and DRP?
b) Who takes care of their implementation?
c) Do you have a team to manage disruptions?
d) What kind of expertise do they have?
e) What is the size of the BCM team or how many individuals are responsible for managing disaster recovery?

II Communication and embeddedness

a) How are BCM and DRP communicated in the organisation?
b) Does the staff in different departments know about DRP?
c) Is there a formal role of BCM in the organisation where there is continual reporting to senior management?
d) Are the employees committed to BC policies and do they execute them?

III BC planning and Processes

a) How does the top management support the BCM and DRP?
b) How does the top management take part in planning of DRP and BCP?
c) How are the critical business functions prioritized?
d) Is the IT infrastructure outsourced?
e) How does BCM consider suppliers and customers?
f) How is information security handled when the company contacts with external organizations?
g) If the external companies have access to internal IT systems, how is information security handled in that case?
h) Do you have SaaS (Software as a Service)? How do you manage security in that case?
i) What do you think is the most critical process/function in your organisation in terms of risk tolerance?

IV Attitudes and ownership

a) Are there any personal incentives to carry out BCM and DRP in the organisation?
b) Is there an Information security responsible in every business function?

V Disruptions

a) How does your company handle disruptions?
b) What kinds of measures are taken to cope with a disruption?
c) Does your company have a BCP or DRP?
d) What is the role of ISsec in BCP and DRP?
e) How vulnerable would your data be in the case of a disruption?

VI Configuration and metrics

a) Does the company manage their own DRP?
b) Do you have the IT infrastructure, the personnel, the knowledge and capabilities and other internal resources to manage disruption?
c) Do you have a contracted reserved supplier for crisis?
d) Do you have on-site (backup), off-site (hot/cold/warm) recovery capabilities? Specifically backup systems managed outside the company premises.
e) How long would it take for the critical processes to resume normalcy after an interruption?
f) If an alternate process runs successfully during a sizable disruption, will it be adequate enough to replace the main business critical process for that time?

VII Legislation and standards

a) Does your company comply with any BC standard?
b) Do have any added incentive to conform to these standards?
c) Do you simply follow BC standards or they have a wider scope in the organisation?

VIII Strategy

a) Do you see the implementation of BCM or DRP as a competitive or strategic advantage or just as a business enabler?
b) Does the BCM improve the development of the organization?