The Evolution of Business Continuity Management in large Irish enterprises between 2004 and 2009

David. N. Garrett BA

Submitted for the degree of Master of Business Studies

Supervisor: Dr Caroline McMullan
DCU Business School
Dublin
Ireland

Date of Submission: May 2012.

DUBLIN CITY UNIVERSITY BUSINESS SCHOOL

DECLARATION

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of Master of Business Studies is entirely my own work, that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed:

I.D. Number: 58127453

Date:

ACKNOWLEDGEMENTS

There are a number of people I wish to thank for their help and contributions during the course of this investigation.

Firstly I would like to acknowledge the guidance, supervision, suggestions, help, friendship and comments provided by my supervisor, Dr Caroline McMullan both before and throughout the course of my postgraduate studies. I want to thank Mr Michael Conway & Mr Colin Delaney for their assistance in the early stages of my research.

I want to thank the Irish Stock Exchange for sponsoring my studies and for their help with the research.

Finally special thanks go to my friends and family for their help and support, you know who you are. I appreciate all you have done for me and can sincerely say I would not have got this far without you.

TABLE OF CONTENTS

ABSTRACT

The Evolution of Business Continuity Management in large Irish enterprises between 2004 and 2009

Mr David Garrett.

The research surveys large Irish enterprises in 2004 and again in 2009 with a view to determining how Business Continuity Management (BCM) has evolved during this five year period. Of the fifty two original organizations, forty four were still trading and twenty eight (63%) agreed to participate in the follow up study. In order to explore the findings from the survey interviews were conducted to allow for a more in-depth discussion of the key findings and possible explanations for the various trends identified.

The results of the study show that: responsibility for BCM is firmly placed in the realm of senior and middle management with a low level of directorial involvement; computer viruses/bugs are now viewed as the greatest threat to Business Continuity; loss of telecommunications is the most often experienced disruption; external rather than internal pressures drive most BCM activity; 89% of organizations have a regularly exercised BCP; and BS 25999 has not as yet had a wide impact in Irish organizations.

On the basis of these findings recommendations were made for national policy formulation and regulation and, at an organizational level, for building organizational resilience.

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Today the globalized nature of the business world, the ubiquity of technology use, the increasing variety of threats and risks faced by both organizations and nation states and global financial issues mean that as we move further into the 21st century the range and types of crisis events faced by organizations are likely to grow. Organizations wishing to remain competitive and successful must be protected, through increased resilience, to continue profitably in the event of any serious business interruption. Current management thinking is focused on key objectives such as meeting end-consumer requirements, product availability, and on-time delivery. To survive firms must get the right product, at the right price, at the right time, to the consumer and on a continual basis. In a changing world organizations must prepare and plan to an even greater extent than they traditionally have for all potential threats.

Business Continuity Management (BCM) can enable the continuation of key business processes, whatever the cause of the disruption/crisis/catastrophe, through its holistic approach. Effective BCM can allow organizations to gain an advantage over competitors in today's contemporary marketplace which is dynamic, global, and customer driven. BCM looks at a wider brief than traditional Disaster Recovery which had a narrow technological focus, as it takes a holistic approach to risk and threat management encompassing all mission critical elements of the business.

1.2 The Roots of Business Continuity Planning

The roots of Business Continuity Planning (BCP) lie in Disaster Recovery (DR) which in turn developed from war gaming and scenario planning. In early incarnations of war gaming, the ability to turn bad situations to your advantage was viewed as the reward of good planning.

Sun Tzu (544-496 BC) wrote 'The Art of War', one of the earliest writings on the subject of strategic thinking, and is considered to be one of the greatest influencers on the topic amongst both military and business thinkers around the world. Oriesek and Schwarz (2008) credit Sun Tzu (544-496 BC) for developing the first war game about five thousand years ago, called “Wei-Hai”, meaning “encirclement. “Wei-Hai” was similar to the game of “Go” which is still played today and which was developed around 2200BC.

Sun Tzu (544-496 BC) introduced the concept of scenario based planning and contingency to military thinking. Some of these strategies whilst military focused included concepts such as backups (weapons caches), scenario planning and planning for the unknown. He recognised that strategy is about responding swiftly, flexibly and appropriately to changing conditions. Strategy is foreseeing what is possible (envisaging scenarios), and preparing appropriately. Oriesek and Schwarz (2008) note that in the nineteenth century in Prussia Germany, Baron von Reisswitz introduced scenarios into war gaming by placing the players in particular situations at the start of a game.

1.2.1 Scenario Planning

Scenario planning emerged out of war gaming more as a method for military planning after World War II. The concept of scenario planning using applications such as systems and game theory was used by Herman Kahn as cited in Oriesek and Schwarz (2008) in the 1950s during the “Cold War Era”. Kahn’s reasoning was the genesis of the famous doctrine of MAD, or "Mutual Assured Destruction", which dominated Cold War thinking up to the President Reagan era in the USA.

One of the main aims of scenario planning is to identify trends and uncertainties and using them look at the outcomes of potential future events i.e. think about the unthinkable according to Oriesek and Schwarz (2008).

The usefulness of scenario planning from a business perspective is evident from the work of Pierre Wack in the early 1970s, who worked as a planner for Royal Dutch/Shell. Based on Wack’s work the Shell Group planned for a future in which they would not have access to the vital data on their mainframe computers and, as a result of this, Shell invested in the creation of Information Technology

(IT) backups. It is noteworthy that these early BCP and DR initiatives took place largely in terms of gaining competitive advantage. Wack (1985) realised that by looking at and being aware of the numerous possible futures an organization could face rather than relying on forecasts based on historic data and by realising that the future was likely to be unstable one could prepare different strategies to address potential issues and challenges of the future.

Oriesek and Schwarz (2008) warn about the limitations of scenario planning noting that it is fundamentally biased by the views of the person or people, who developed the scenario in the first place and therefore is limited to the extent of their imagination. They also note that, depending on the approach taken, scenarios can be nothing more than rational and safe extensions of the past and often classify likely outcomes along simple linear views of reality, whereas the real world involves complexity and multiple dimensions.

The development of future scenarios did however enable organizations to realise how reliant they were on their IT systems and the data they held. The realisation that systems needed protection formed the requirements for early DR planning.

1.3 Disaster Recovery to Business Continuity Planning

Business Continuity Planning (BCP) has its roots firmly in DR planning, which emerged in organizations during the 1950s and 1960s.

> “The origins of the word “disaster” are from the Latin for “bad star” (*dis*+ *astro*). Disasters were originally perceived as resulting from malevolent astral influences… The purpose of “disaster recovery” is to respond to disastrous events, usually through the preparation of contingency plans, not to seek to prevent them.” (Swartz, E. Elliott, D. and Herbane .B. 1995, p. 17)

Herbane (2010) refers to the fact that companies began to store backup copies of their critical data, paper or electronic, at alternate sites. DR in the main originated from the wish of US banks to better protect their corporate data centres. The goal of DR was to protect the technical systems rather than providing any organizational/business side protection. Out of DR scenario planning the idea of having backup or recovery sites arose. At first this offsite storage happened only periodically, but file backup and offsite storage procedures became more frequent and regular by the late 1970s, also around this time third-party regional storage facilities were created to form what would become the alternate site, or “hot site”.

Over the decades DR has evolved into BCP and then on to Business Continuity Management (BCM). This evolution is best characterised by a series of mind-sets outlined by Elliott, Swartz and Herbane (2010).

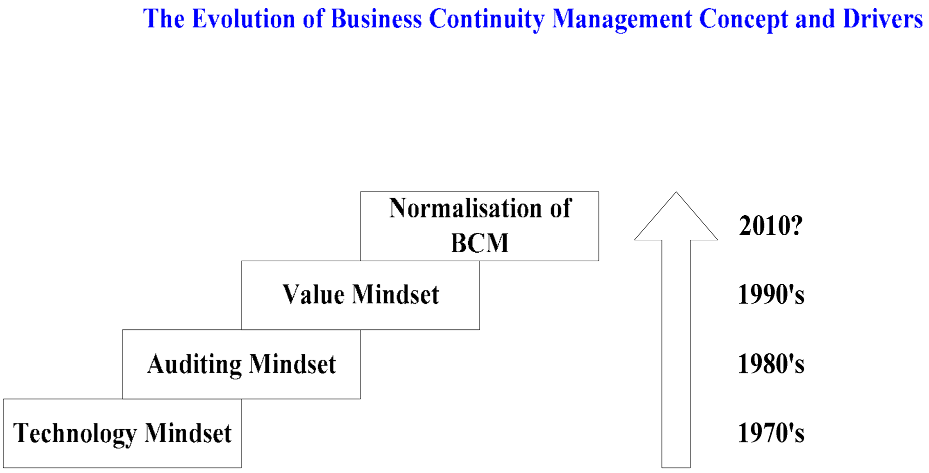


Figure 1.1: The Evolution of BCM Concept and Drivers (Elliott, Swartz and Herbane, 2010, Figure 1.2, p. 14)

1.3.1 Technology Mind-set

This basic DR approach focused purely on the technical aspect of recovering from disasters and assumed that disasters were triggered by technology failure and was not expanded beyond this to look at the wider business causes of disasters according to Elliott, Swartz and Herbane (2010).

> “The internal and hardware focus of disaster recovery permits only partial examination of the causes of disasters and seeks to treat their effects or symptoms rather than to prevent them.” (Swartz, Elliott and Herbane 1995, p.15)

In the late 1970s and 1980s DR was broadened to include a wider base, creating the BCP approach which looked at wider internal factors which had a bearing on crisis events in an organization. This expansion happened because the nature of IT systems changed from a mainframe centred data processing approach to a more End User Computing (EUC) approach as outlined by Panko (1987). The move to EUC spread computing across organizations and had a significant impact on DR as company data was now dispersed rather than centralised; as was previously the case with the mainframe approach. This EUC change was noted by Elliott, Swartz and Herbane (2010) alongside the realisation that BCP was also another form of insurance.

> "The emergence of personal computers during the 1980s and the diffusion of control of IS among organiszations (Panko, 1988) provided a basis for developing an auditing mindset in which a task for central IS departments was to regulate and police." (Elliott, Swartz and Herbane 2010, p.16)

This move from the pure DR approach to a BCP approach is referred to by Elliott, Swartz and Herbane (2010) as the 'Auditing Mind-set'.

1.3.2 Auditing Mind-set

The auditing mind-set, while still focusing on technology expanded its focus to include the protection of business activities also and was mainly driven by external regulation. Rather the relying on the 'mind-set' approach to BCM, Herbane (2010) outlines an alternate four phases based around regulation and legislation. While these phases are distinct there are some overlaps between them.

> "The four phases are emerging legislation and its arrival by stealth (mid-1970s to mid-1990s), emerging standards and broader influence (mid-1990s to 2001), the post-9/11 landscape – acceleration and focus (2002–05), and internationalisation – competing standards and breakout (2006–10) (Herbane 2010, p.979)".

In 1997, Herbane, Elliott and Swartz recognised the major shift from traditional DR to BCP. The BCP approach was much broader than DR and looked to prepare for incidents that might disrupt all business activities in an organization. BCP helped to identify and understand the often complex causes of business disruption and it was noted that a gain in organizational competitive advantage was possible as a result of having BCP as a central business process.

The auditing mind-set approach however did not take into account the impact of the human contribution to disruption events or of the human influence on the impact of the BCP process. The key focus of the auditing mind-set was concerned with how to prevent and survive any disruptive event and on how to engineer compliance.

The transition from DR to BCP was described by Herbane, Elliott and Swartz (1997) as being part of a continuum that allowed organizations to judge where they were positioned. Such a continuum is shown in Figure 1.2.

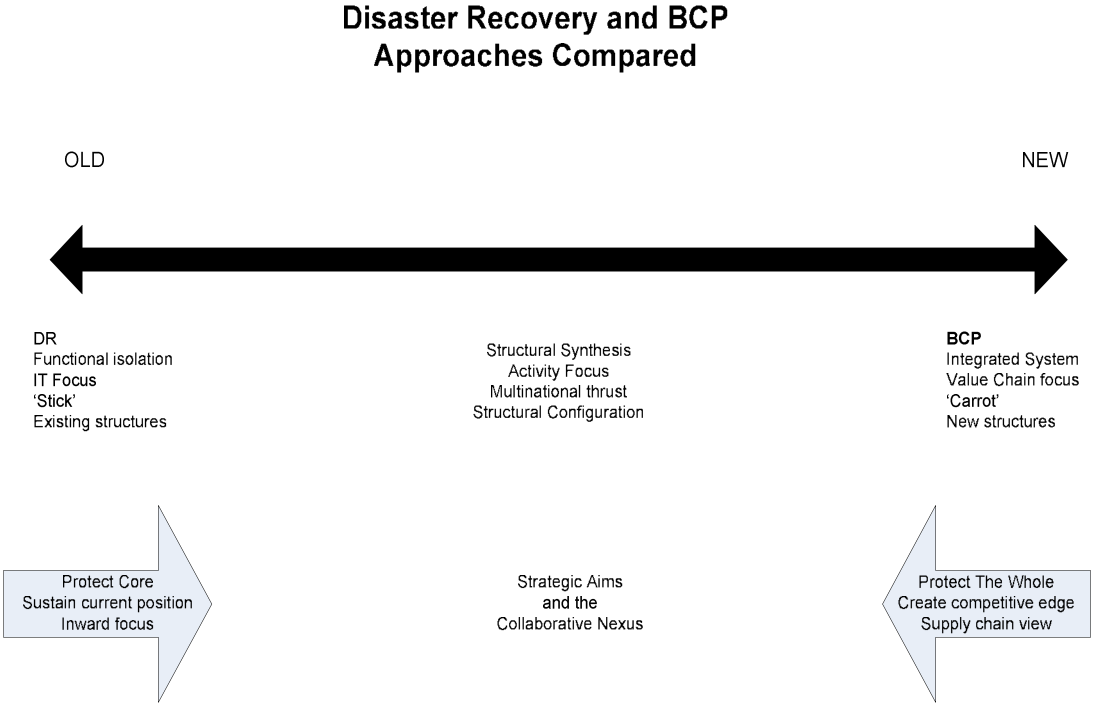


Figure 1.2: Disaster Recovery and BCP Approaches Compared
(Herbane, Elliott and Swartz 1997, p.20)

The 'auditing mind-set' covered BCP until the mid-1980s when a broadened scope created BCM and the value based mind-set. That is not to say that the auditing mind-set has disappeared. It persists in some organizations, most often those driven by compliance to regulation.

1.4 BCP to Crisis Management and Business Continuity Management

Moving further into the late 1980s and into the 1990s the area of BCP was expanded to take into account external factors by taking its cues more from Crisis Management (CM).

> "Crisis management is the organisation and coordination of activities in preparation for, and response to, events that prevent or impede normal organisational operations (thereby threatening its most important goals) ."
> (Herbane 2010, p. 979)

The CM approach to BCP differs from the initial, internal and preventative focused BCP and DR approaches and deals with both prevention and recovery.

Mitroff (2001) noted that the origins of crisis events are built into all organizations and societies or anything that is a complex system and while we may not be able to stop crises happening they can be managed with practice. Mitroff (2001) also noted that while crisis may be rare and unforeseen they can be managed:

The CM approach to BCP also identified, according to Swartz, Elliott and Herbane (1995), that there is a complex interaction of system elements that need to be recognised, that DR approaches did not seek to prevent the threats and that crisis had both internal and external elements.

The emphasis of CM is on preventing crisis rather than curing the causes. As outlined by Swartz, Elliott and Herbane (1995), a crisis has a minimum of three phases that includes, a pre-incident phase, the focal incident and a post-incident phase of recovery and turnaround. They further note that disaster recovery approaches focus on the latter two stages while crisis management places special emphasis on prevention in the pre-incident phase.

The 'crisis management' approach is incorporated into the 'Value Based mind-set' as put forward by Elliott, Swartz and Herbane (2010), which concentrated more on the potential for expanding BCP to add more value to the organization as a whole and to broaden out its focus to include all organizational stakeholders. This new expanded focus created the BCM approach. The BCM approach with its more inclusive organization wide and external considerations should provide better forecasting and protection from disaster events that befall the organization.

None of the approaches outlined guarantee 100% successful recovery when an incident occurs. Regardless of the approach taken, there is still a likelihood that a sequence of events will occur that will result in a disaster scenario, but by adopting a BCM approach the ability of an organization to be resilient and to have the ability to recover and continue working after a disaster are enhanced.

1.4.1 Value Based Mind-set

The 'values based mind-set' moved BCP towards BCM and was described as:

> "Concerned less with compliance, regulations or technological failure than with the business itself. Crucially, in this mindset BCM is regarded as having the potential to add value to the organization, not just consume revenues." (Elliott, Swartz and Herbane 2010, p.18)

In this mind-set the scope of BCP is broadened to include the whole organization, including employees who are recognised by Elliott, Swartz and Herbane (2010) as the biggest challenge in implementing and managing the BCM process. Organizational stakeholders were also recognised as an important driver for change and hence for the introduction and development of BCM. BCM is a combination of social and technical systems that together make for effective BCM and should permeate everything an organization does. It can be seen as a value adding process due to the fact that it should result in more efficient systems and better customer value through better responsiveness, reliability and security.

The danger of focussing BCM on too narrow a technical area is still to the fore in the academic literature. Chadwick (2001) and Myers (2006) both point to the danger of the protection of systems becoming the objective of BCM rather than a more holistic approach being taken. A balance between the technical and business focus is still relevant today as businesses become ever more reliant on technology.

1.5 Business Continuity Management within Organizational Resilience

It is recognised that in order to ensure organizational resilience (OR), BCM which is an element of OR has to take into account the human, organizational and social aspects of the organization's environment. This expanded view of BCM moves it further into the realm of OR.

The importance of BCM cannot be over emphasised, not only in terms of the organization internally but also to the external operating environment of the organization such as its supply chain both up and down stream. Coles and Buckle (2004) identify the multiple dimensions of resilience and highlight the importance of participation by the affected communities in the recovery process. National Governments have also come to recognise the importance of BCM particularly since 9/11 with regards to the resilience of their countries. The 9/11 attacks on New York City have been identified by Herbane (2010) as crucial events regarding BCM:

> "The terrorist attacks of 11 September 2001 also marked a change in BCM practices to incorporate the notion of enterprise/organisation wide resilience in which there are shared notions about resilience by employees and greater flexibility in the plans developed to respond to large-scale disaster scenarios." (Herbane 2010, p.984)
>
> And
>
> "The post-9/11 landscape can be characterised by a notable acceleration in the introduction of guidelines and regulations for organisations operating within the financial services sector, public authorities, stock exchanges and utilities." (Herbane 2010, p.987)

The UK government under the Civil Contingencies Act (2004) gave Local Authorities the duty to provide businesses and voluntary organizations with advice on BCM. This duty aims to ensure local businesses are able to more quickly recover from disruptions and that all category one responders have a business continuity management plan in place. The idea behind this legislation is that a resilient business community helps to create a resilient country.

While it is recognised that BCM needs to be an organizational wide process which is included at each stage of all the organizations processes, current thinking moves BCM further under the umbrella of OR, an all-encompassing approach including Risk, Security, Emergency and BC management.

In order to achieve OR, organizations need to move beyond BCM or Risk Management and develop a concept of resilience. Cummings (2003) notes that a culture of continuity is required across an organization in order for it to be prepared. OR views an organization as similar to the concept of a living organism that has to be adaptable in order to respond to the challenges it may face according to Ellwood (2009). To better understand what is meant by resilience Riolli and Savicki (2003) cite a definition by Horne and Orr (1998):

> "Resilience is a fundamental quality of individuals, groups, organizations, and systems as a whole to respond productively to significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behaviour." (Riolli and Savicki 2003, p. 227)

The concept of OR is not a new one and was recognised in the late 1990s as being on the horizon of thinking in the area of BCM. Horne III (1997) outlines that OR is the ability of a system to withstand the stresses of environmental "loading" based on the combination/ composition of the system pieces, their structural inter-linkages, and the way environmental change is transmitted and spread throughout the entire system. Horne III further states that to varying degrees, resilience is a fundamental quality found in individuals, groups, organizations, and systems as a whole. It allows a positive response to significant change that disrupts the expected pattern of events without resulting in regressive/non-productive behaviour. A shared sense of purpose/mission and planning are also vital factors in achieving OR. He also identifies IT as playing a vital role and notes that the organization needs to be aware of its competencies and the challenges it faces.

The concepts of OR as a process to help organizations survive crises and volatile economic shifts is further expanded by Riolli and Savicki (2003):

> "The concept of the "resilient organization" has gained popularity as a concept that might aid organizations survive and thrive in difficult or volatile economic times.
>
> At the organizational level, characteristics of organizations (e.g. human resource practices, organizational culture and values) have been related to nimble reactions and continued survival under volatile, demanding, and

> dismal work conditions…We believe,… that resilience in organizations builds on the foundation of the resilience of members of that organization. We also believe,… that resilience at the individual level does not guarantee resilience at the organizational level. Both levels must be addressed." (Riolli and Savicki 2003, p. 228)

Riolli and Savicki (2003) further allude to the fact that adaptability is a key component in surviving adversity.

According to Horne and Orr (1998), as cited in Riolli and Savicki (2003), OR is made up of seven organizational behavioural streams (community, competence, connections, commitment, communication, coordination and consideration). They also contend that the only constant faced by organizations today is change. This change needs to be countered by having a flexible organizational culture that is adaptable. Observing that true resilience relies on organizations addressing both tangible and intangible elements, Ellwood (2009) recommends selecting the correct guidance in building OR is fundamental to success and advocates using the BS25999 standard for Business Continuity Management as a guide.

The evolution from DR to BCP to BCM and then BCM on to being a part of OR has gradually occurred over the last 40 plus years. As mentioned earlier, BCM is not just about reacting to an incident or just about DR, CM, RM or technology recovery. BCM is a business owned activity that can give an organization a framework to review the way it provides products and services and increase its resilience to disruption, interruption or loss.

1.6 Research Objectives

As stated by Kelly and McMullan (2011), there is a dearth of research into how organizations implement BCM. The intention of this research is therefore to add to the body of knowledge on BCM and its implementation.

The primary objective for conducting this study was to examine the evolution of BCM in large Irish enterprises between 2004 and 2009. This research builds on an earlier survey completed in 2004. BCM was not new in 2004 yet the extent of its practice in large Irish organizations had remained uncertain in the absence of investigation and research. Little research has emerged since the original study so the decision was made to replicate the survey with the same organizations five years later.

The research question posed was: How has BCM evolved in large Irish enterprises between 2004 and 2009? To answer this research question the following research objectives were identified:

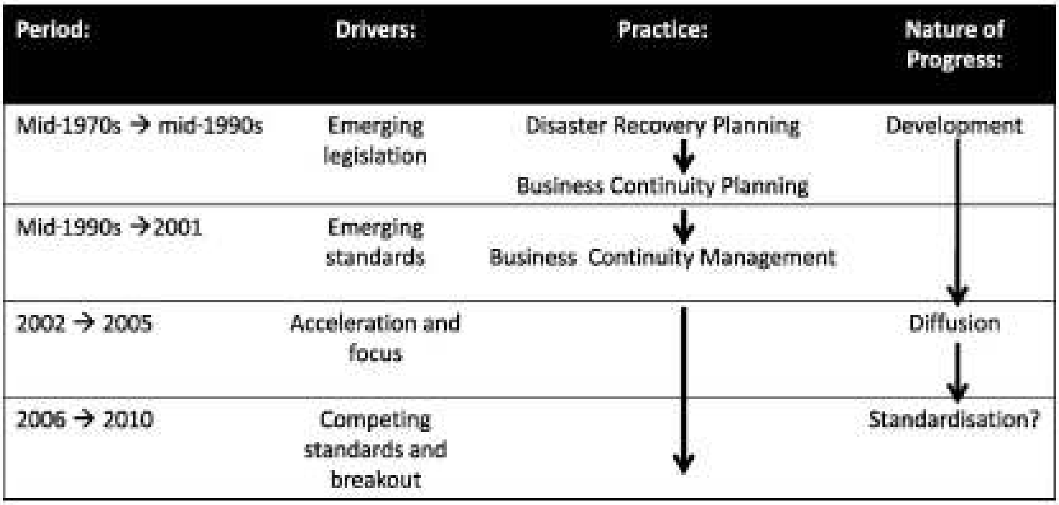
1. To explore what constitutes BCM;
2. To analyse current research in BCM, with particular emphasis on what constitutes good practice in the area of BCM;
3. To identify how BCM theory has developed and evolved;
4. To replicate the 2004 survey with the same organizations;
5. To analyse and interpret the results of the 2009 survey against those of 2004;
6. To conduct interviews with industry experts to validate the survey results;
7. Finally, to form conclusions as a result of the above analysis.

1.7 Structure of the Thesis

This thesis is comprised of six chapters. Chapter two presents a review of relevant literature on BCM. The particular focus of this chapter is to present the current "state of the art" regarding best practice in BCM. It uses the Business Continuity Lifecycle as the framework around which the review takes place and cites wider general management literature where appropriate. Chapter three provides an account of methodological issues considered in the design and execution of the study. In particular it examines the data required to answer the research question; the data collection methods employed and the approach to data analysis which was utilised. The results of this research are presented in Chapters four and five. Finally, Chapter six includes a discussion of the results of this research, and recommendations for building organizational resilience. The strengths and limitations of the study are also considered and some directions for future research are outlined.

1.8 Conclusion

As organizations move further into the 21st century, the range and type of business interruptions are likely to increase as the spread of technology grows. Organizations need to consider the challenges posed by developments in the political, economic, social and technological environments. BCM as a discipline is maturing and needs to be approached by organizations in a holistic manner which acknowledges the contribution which BCM can make towards achieving overall resilience. Good practice involves seeing BCM as a strategic issue that encompasses all of the organizational stakeholders rather than focusing on technology alone as in the past. The world of business has undergone many stages in its development and BCM is no different. The impact of legislation, regulation and standards are forcing organizations to focus their efforts onto BCM, as represented by Herbane (2010).



Period:	Drivers:	Practice:	Nature of Progress:
Mid-1970s → mid-1990s	Emerging legislation	Disaster Recovery Planning ↓ Business Continuity Planning	Development ↓
Mid-1990s →2001	Emerging standards	↓ Business Continuity Management	↓
2002 → 2005	Acceleration and focus	↓	Diffusion ↓
2006 → 2010	Competing standards and breakout	↓	Standardisation?

Figure 1.3. The development of business continuity management: periods, drivers and practices (Herbane 2010, p. 992).

This chapter has introduced the study which is presented in this thesis. It has explained the motivations for the study, articulated its objectives, outlined the historical evolution of BCM and presented the structure of the thesis. The next chapter presents the literature review.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This literature review on Business Continuity Management has been structured around the stages of the Business Continuity Lifecycle which consists of: BCM Programme Management; Understanding the Organization; Determining BCM Strategies; Developing and Implementing a BCM Response; Exercising, Maintaining and Reviewing; and Embedding BCM in the Organizational Culture. Before moving into this review, the chapter begins with an exploration of what constitutes BCM.

The research also includes an analysis of the impact that Organizational Resilience (OR) has had on BCM as there has been a distinct move in the literature to broaden the BCM perspective and to look to combine it with other disciplines such as risk, crisis and emergency management to create a more comprehensive approach leading to enhanced OR.

2.2 BCM a definition

The evolution of business continuity management from Disaster Recovery (DR) to Business Continuity Planning (BCP) to BCM as outlined in Chapter One has led to many different definitions being proffered over time. Elliott, Swartz and Herbane (2002) diagrammatically represent the evolution of BCM starting with DR through to BCP to BCM and into the future. This diagram shows the link between these processes and their evolution.

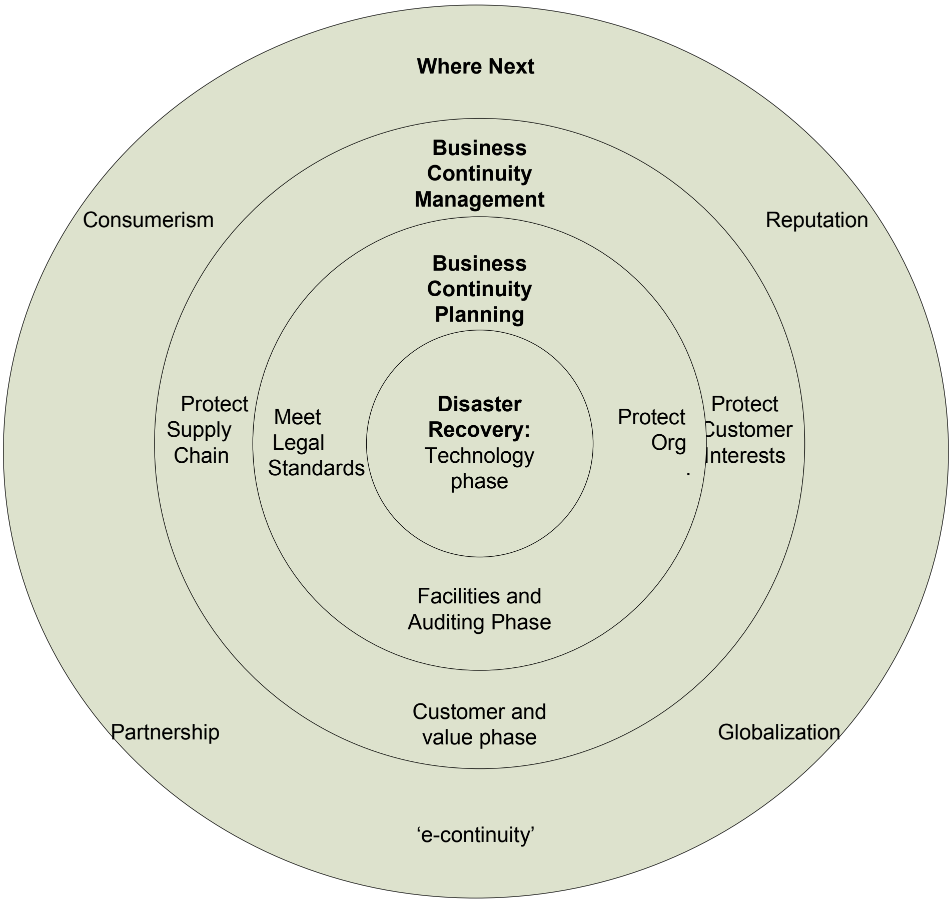

Where Next
Business Continuity Management
Consumerism
Reputation
Business Continuity Planning
Protect Supply Chain
Meet Legal Standards
Disaster Recovery: Technology phase
Protect Org
.
Protect Customer Interests
Facilities and Auditing Phase
Partnership
Customer and value phase
Globalization
'e-continuity'

Figure 2.1: Augmenting business continuity
(Elliott, Swartz and Herbane 2002, Figure 7.2, p.188)

2.2.1 BCM

Herbane (2010) states that, BCM has become established as a formalised structure and expression of an organization's crisis management values and practices with standards developed in the early 2000s. BCM focuses on assuring continuous business processes and plays a prominent part in the organizations ability to recover after disruption. BCM is also an on-going process and planning for it includes reviewing DR, business recovery, business resumption and contingency planning. The comprehensive and on-going nature of BCM should therefore be included as part of any BCM definition.

Research conducted by Elliott, Swartz and Herbane (2010) suggests adopting a crisis management approach to BCM. They suggest expanding the process of BCM to include the social elements that are often part of a disruptive event and maintain that organizations often play a role in causing failures themselves. They also note the important role that an organization's managers play in BCM, the fact that interruptions impact on the many stakeholders in an organization and that if managed properly incidents do not necessarily inevitably lead to a crisis. This means that the wider supply chain and all an organizations stakeholders both internal and external need to be covered in a BCM definition.

The Information Technology Infrastructure Library (ITIL), IT Service Management framework offers an alternate risk management view of BCM saying that it is the business process responsible for managing risks to the business and that it protects the interests of key stakeholders, organizational reputation, brand and value creating activities.

The ITIL definition also notes that BCM helps reduce risks to an acceptable level. It is interesting to note the business focus of the ITIL definition as ITIL is mainly a technology focused process. The ITIL definition further shifts the focus of BCM away from technology and on to the business and its stakeholders. The Basel committee on banking supervision, taking a financial and business focus, define BCM as:

> "A whole-of-business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption." (Basel Committee on Banking Supervision, 2006, p.1)

The BCI note that BCM and risk management sit side by side and that the main objective of BCM is to allow organizations manage their business under adverse conditions by implementing resilience strategies, recovery objectives, BCM and crisis management plans in collaboration with, or as a key component of, an integrated risk management initiative.

Ultimately the most comprehensive definition of BCM which aligns with the current BCI definition and includes the multiple elements covered by the earlier definitions posed by academics, is that put forward by the standard British Standards Institute (BSI) which states that BCM is:

> "A holistic management process that identifies potential threats to an

> organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities." (BSI 2006, p.1)

This definition notably recognises that BCM is a part of building an overall OR based approach to disruptive events and it encapsulates the main elements of earlier definitions such as resuming business after a disruptive event, the survival of the mission critical elements of the business, the ability to prepare for disruptive events, the continuous nature of BCM, testing/rehearsing BCM, the internal/external nature of events and the competitive advantages gained thru OR as a whole.

BCM as noted by Herbane (2010) which began as an Anglo-centric, information technology focused activity has become a process that has now become an expectation rather than luxury.

2.3 The Literary Framework

The framework around which the literature is reviewed is drawn from the BCM lifecycle, which sits at the centre of The British Standard for Business Continuity, BS25999, and captures the key themes as reflected in the academic literature. A key aim of the literature review is to identify and discuss what has been proposed as constituting good practice in terms of BCM. This is then used as the benchmark against which the research can measure the execution of BCM in large Irish organizations. The lifecycle is illustrated in Figure 2.2.

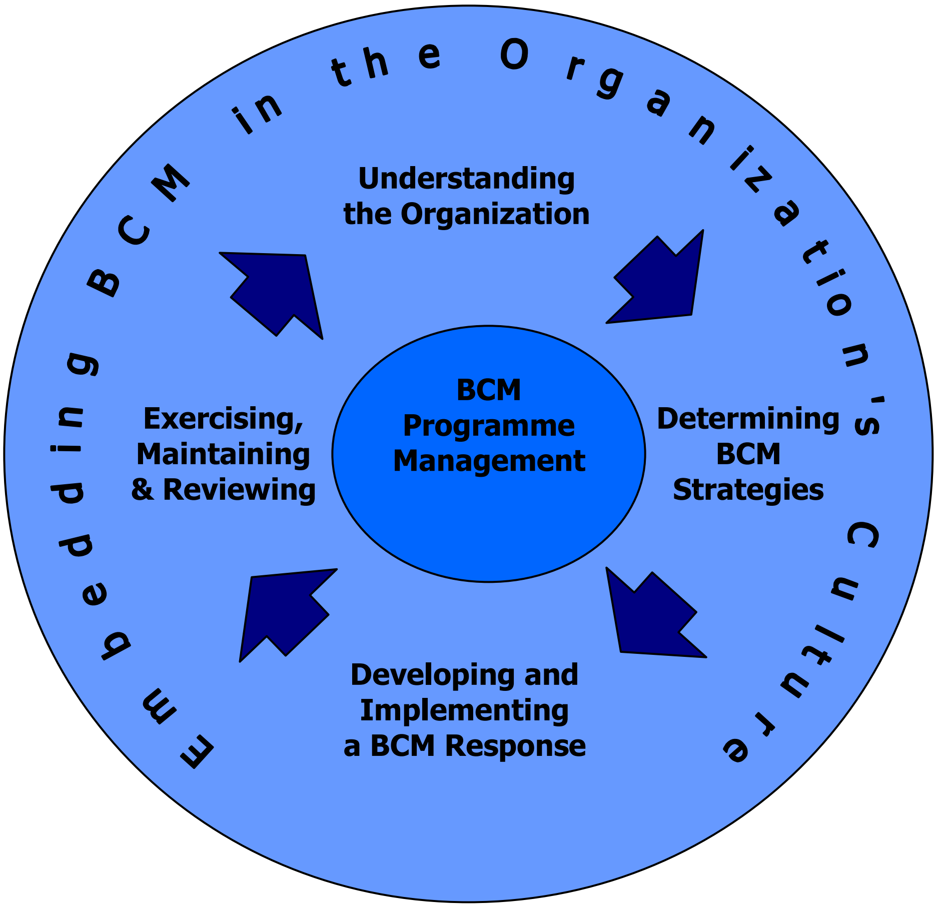

Embedding BCM in the Organization's Culture
Understanding the Organization
Determining BCM Strategies
Developing and Implementing a BCM Response
Exercising, Maintaining & Reviewing
BCM Programme Management

Figure 2.2: The Business Continuity Management Life cycle
(BSI 2006, Figure 1, p. 9)

Hence forth referred to as The Standard, BS25999 provides a basis for understanding, developing and implementing business continuity within an organization. Developed by a broad range of experts and industry professionals, The Standard is designed to suit any organization, large or small, from any sector. Each of the six elements of the BCM Lifestyle will be used to guide the literature review.

- BCM Programme Management.
- Understanding the organization.
- Determining business continuity strategy.
- Developing and implementing a BCM response.
- BCM exercising, maintaining and reviewing BCM arrangements.
- Embedding BCM in the organization’s culture.

2.3.1 BCM Programme Management

Programme management is central to the BCM process and includes:

- Ensuring participation of top management;
- Assigning responsibilities (Governance);
- Implementing business continuity in the organization;
- The on-going management of business continuity.

2.3.1.1 Participation of Top Management

When reviewing the body of literature it is evident that the participation of senior management is crucial to the success of BCM. Seow (2009) points out that not getting top management buy in and commitment to starting and sustaining a BCM programme in an organization can be an obstacle to the programme's success. Without it the BCM programme will almost certainly fail. It is the responsibility of the board of directors to review the business continuity programme annually according to Koch (2004). Directors have a fiduciary duty to protect corporate assets and safeguard the long-term survival of the organization. If the board does not play an active part in BCM, sustaining a programme will be difficult.

The literature identifies the need to strategically sell BCM to senior executives and to contextualise it by showing them its importance to the organization. As noted by Seow (2009), selling BCM to senior executives is important. Seow (2009) advocates that this is achieved not just by using business models to illustrate the returns on shareholder value, citing statistics on the number of companies without business continuity plans (BCPs) that failed after a disaster event and providing case studies of past incidents, as these tend to be generic and superficial. Such approaches often fail to motivate senior executives into engaging with BCM. To attract the attention of senior executives, Seow (2009) advises that where possible the BCM leader needs to make the case for BCM by presenting it in the right management context that has direct relevance to the senior executives personally.

Looking further towards raising senior management awareness of importance of BCM, Lindstedt (2007) points out that executives cannot be expected to support a BC programme if they consider it as simply part of another function of the business, like risk management. The BCM practitioner therefore needs to find out what are the priorities of senior management? What stakes do they have in supporting or not supporting BCM? What motivates them? How can these priorities be leveraged?

According to De Waal (2006), disasters that resonate in the moral imagination elicit responses. De Waal (2006) notes that there are four political components of disaster prevention: the visibility of the disaster; the political salience of the disaster; the constituencies affected and involved in the response; and the availability of technologies for effective response. These need to be borne in mind when trying to get the required positive management response regarding any BCM initiative.

In delivering the BCM message and trying to illicit the required senior management response, it is important to note that most people are influenced more by one clear, vivid personal example than by an abundance of statistical data according to Aranson (1999). The BCM message needs to be delivered by a credible communicator. Myers (2006) also advocates that the person with BCM responsibility needs to ensure BC is positioned correctly which means positioning and selling senior management on a corporate contingency planning policy and strategy, and documenting this policy and strategy in writing before any other activities are undertaken in the programme process.

Getting board commitment is the first step in starting a BCM programme according to Gallagher (2003) who also advices that BCM responsibility should not be given to someone as an add-on to their existing role or just for something to do. From this process a BCM sponsor should emerge who will champion the programme.

General management literature by Aranson (1999) argues that in order to increase the effectiveness of communication it is important for those advocating BCM to senior management to recognise the three variables at play when communicating:

1: the source of the communications (who says it);
2: the nature of the communication (how they say it);
3: characteristics of the audience (to whom they say it).

The literature highlights that in any BCM programme it is vital to receive input and commitment from the Chief Executive Officer (CEO) from the very start, particularly at management kick-off meetings. Barnes (2001) makes reference to this by saying it is important that the plan that will be written is the CEO's plan to get the organization operational again after a major disaster. The support for BCM from the CEO must also be on-going. As Elliott, Swartz and Herbane (2010) point out, the BCM process normally needs senior management support and progress should be regularly reported to the senior management team. Senior management play a vital part in BCM by deciding where the focus of business continuity provision is to be and also in determining the mind-set that will drive business continuity management from a strategic perspective.

The impact of corporate governance and regulatory issues on senior management further highlights the importance of senior management participation and backing any BCM programme. As noted by O'Hehir (2007), corporate governance is in place to balance and manage risk and implement internal control procedures on entrepreneurial energy. O'Hehir (2007) further outlines that directors and senior management are obliged to provide assurances on corporate governance to both regulators and stakeholders and must keep themselves informed of organizational risks and obligations. It is important to recognise in relation to regulation and its imposition, as noted by Elliott, Swartz and Herbane (2010) that controls that come from outside the organization are usually imposed as the authority implementing them will probably have statutory powers to enforce compliance. It is therefore better for an organization to address BCM issues itself rather than having them forced upon it by external regulators.

Involvement in BCM programmes on an on-going basis should therefore be a normal part of senior management's role as it would with operational risk management for instance. Knowledge of senior management priorities and issues will enable the BCM practitioner to get the required backing for the BCM programme in order for it to be established on a firm footing.

The next important step in the BCM programme after gaining management approval and backing is to make sure that the programme responsibilities are correctly assigned to the relevant groups and individuals.

2.3.1.2 Assigning Responsibilities (Governance)

When assigning responsibilities for the BCM programme the literature clearly states that those responsible need to have the required levels of authority and seniority in order to make the programme successful, responsibility should not be given to a member of the IT team as the danger will be that BCM will be looked on as an IT initiative by the rest of the organization. All levels of the organization should be involved in the implementation of BCM.

The Standard, highlights that an organization should appoint someone with the appropriate seniority, authority and skills to be accountable for its implementation and should appoint a team or group to implement and maintain the BCM programme. It is noteworthy that the emphasis is on an individual with the appropriate seniority and authority and that a team rather than one individual is responsible for implementing and maintaining the plan. Aronson (1999) also recognises that one of the most crucial steps when assigning responsibilities for a BCM programme is that the correct person with the required levels of authority is chosen to head up the programme.

To enable the BCM programmes success it is crucial that responsibilities are not split across to many groups or departments but are focused in the appropriate areas. Organizations still tend to split BCM responsibilities between operations, security, IT, management, and other departments, thereby increasing the risk that something will fall through the cracks according to Adkins, Thornton and Blake

(2009). Elliott, Swartz and Herbane (2010) warn that the BCM project management role should not be given to an IT specialist either as this then makes BCM an IT issue and not a business wide issue and advise that the board appoint a business continuity steering group to support the BCM project manager in order to drive the process at local or departmental level. The steering group should include senior and influential staff from different business units or departments and acts as a conduit between operative level employees and any central BCM team. The involvement of employees in the BCM programme as highlighted by the Standard, states that it may be appropriate to select representatives from across the organization by function or location to help implement the BCM programme and advocates that BCM roles, accountabilities, responsibilities and authorities should be integrated into job descriptions and skill sets. To reinforce these responsibilities they must be included in the appraisal and reward system of the organization. Once the correct responsibility for BCM has been identified the implementation of the programme is the next logical step.

2.3.1.3 Implementing Business Continuity in the Organization

The activities which need to be undertaken when implementing the BCM programme or indeed any programme in an organization include the design, building, and implementation of the programme. The literature states that a proper project management framework should be used to ensure the programme is effective. Designing and building BC plans, and keeping them updated in a large organization can be a daunting task according to Howe (2007). He advocates that proper project reporting relationships are used throughout the initial BCM project and on an on-going basis to ensure the process is integrated into corporate processes.

The Standard recommends that the organization should implement BCM using a standard project management methodology e.g. PRINCE2 or PMI's PMBOK, to make sure that the implementation is completed in the most effective manner. When considering the phases of a BCM project, various approaches are advocated all of which contain similar project management phases.

Barnes (2001) identifies the main phases as being, project foundation, business assessment, strategy selection, plan development, testing and maintenance. Elliott, Swartz and Herbane (2010) refer to the continuity management process as having four distinct phases namely, initiation, planning for business continuity, implementation and operational management. Howe (2007) maintains that a BCM project can be broken down into three phases, information gathering, plan development and the transformation phase where the BCP project becomes an on-going corporate-wide process. Regardless of the BC plan formation process used, Ginn (1992) notes that the resulting BC plan needs to be modular in design so that it can be easily updated and broken down into readable sections as not all disasters will be major ones. Once the BCP plan is in place the issue of its on-going management needs to be addressed.

2.3.1.4 On-going Management of Business Continuity

As evidenced from the literature on a regular basis senior management should communicate the importance of the BCM programme to the whole organization and appropriate stakeholders in order to keep it in focus. Appropriate BCM training should take place for all staff and senior management must ensure that the BC plan is kept as a living document. BCM should ensure that systems and plans are updated whenever there is a significant change in the organization's environment, personnel, processes or technology. BC plans also need to be updated when an exercise or incident highlights deficiencies.

According to Brazeau (2008), everyone within an organization must embrace BCM for it to be effective. As noted by Elliott, Swartz and Herbane (2010), effective BCM is a part of sound management practice and not a bolt on process.

In order to ensure that BCM is kept up to date it is crucial that it is embedded into the organizations culture beginning at the top of the organization and working its way down through it using continual communication so that it will become part of the way that an organization is managed. At each stage of the BCM process, opportunities exist to introduce and enhance an organization's BCM culture to ensure this happens.

De Witte and van Muijen (1999), present a conceptual model of the different elements that should be taken into account when dealing with organizational culture. Influences on an organizations culture are wide and varied and include the overall national culture, business environment, stakeholder influences, internal vision of the organization, its own processes and goals and the organizations relations with its employees.

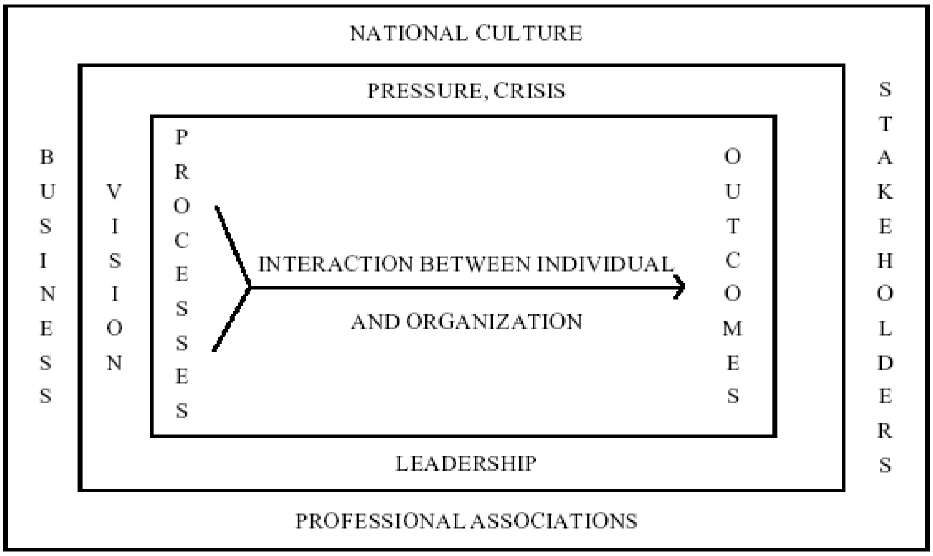


Figure 2.3: A conceptual model for understanding organizational culture. (De Witte and van Muijen 1999, Figure 1, p. 498).

2.3.1.5 Understanding Organizational Culture

When embedding BCM into the organizations culture it is helpful to have an understanding from general management literature of what is meant by organizational culture. Kello (2009) states that most definitions of culture emphasize that culture represents a high-level, sum-total of attitudes, beliefs, norms, and behaviours. In these terms, culture specifies “how things work around here.” Kello (2009) identifies that there has always been a bit of a “chicken-and egg” problem with culture and its measurement which comes first, the behaviours and attitudes, or the culture?

All organization cultures have a number of characteristics according to Luthans (2002), observed behavioural regularities, norms, documented values, philosophy, rules and organizational climate. Luthans (2002) notes that organizations do not have uniform cultures consistently throughout but from a culture management perspective it should be assumed that they have a consistent culture. Culture provides members of the organization with a sense of organizational identity and generates a commitment to beliefs and values that are larger than themselves. It can be interpreted through rites and ceremonies, stories, symbols and the language used in the organization. It should be noted that culture serves two critical functions in organizations according to Daft (2001); it integrates members so they know how to relate to each other and it helps the organization to adapt to its external environment.

It is important to acknowledge as outlined by Kello (2009), that there are often both explicit (what the organization says it is about) and implicit (inferences, often unwritten that the employees draw from their experience in the organization) cultures evident and in operation in organizations. Mitroff, Pauchant, Finny and Pearson (1989) as cited by Elliott, Swartz and Herbane (2010) suggest that an organizations culture is the set of 'unwritten rules' that govern 'acceptable behaviour' within and outside the organization.

Bearing the above in mind is important when considering the impacts of culture on a BCM programme.

2.3.1.6 Culture and BCM

When viewing culture from a BCM perspective, Rossing (2007) states that culture is present in all stages of the process. When auditing/reviewing an organization's BCM process the culture that develops over time should be taken into account. A strong BCM culture will more than likely reflect that the BCM programme has strong senior management support and therefore visible investments in maintaining high levels of resilience. With a weak BCM culture these elements will most likely be missing. Alesi (2008) stresses that when creating a culture of resiliency; accountability needs to be co-located with authority and BCM components should be integrated into day-to-day operations. It is important to make every employee part of a plan, and make the plan accessible to them. The organization must be prepared to improvise. Sheffi (2007) states that when creating a culture of resiliency within an organization where employees are able to respond quickly to incidents using familiar tools, which creates a model that lends itself to the required flexibility, the right corporate culture, "a shared passion to be successful" is a crucial ingredient in creating resilient enterprises.

Addressing the concept of safety culture in particular, Kello (2009) notes that the concept of a safety culture, as an element of the overall organizational culture, has become a prominent part of the research and practice of safety in the workplace. According to Spegener (2009), organizations need to shift the focus of safety performance away from injuries and toward managing and minimizing exposures. The drive to minimise exposures to safety issues will also aid the overall BCM culture as risks will need to be assessed and addressed as part of this process.

Building, promoting and embedding a BCM culture within an organization is necessary to ensure that it becomes part of the organization's core values and effective management. As mentioned by Cummings (2003), for some companies the impetus for this culture comes from outside the organization often in the form of regulatory requirements. Youngblood (2000) suggests that in order to prosper in the 21st century, organizations need a culture that is agile, innovative and has vitality. This allows them to cope and successfully adapted to new business rules. Having an agile, innovative organizational culture will ensure that the BCM programme is kept up to date, current and is embedded in the organization.

The benefits arising from a positive organizational BCM culture as outlined in The Standard are that it will make the BCM process more efficient, gain stakeholder confidence, increase resilience over time and minimise the chance of disruptions. Organization culture will therefore predicate how BCM or any change is handled. As pointed out by Luthans (2002), organizations must have a culture that learns and anticipates change. If the prevailing culture of the organization is reactive rather than proactive and does not have the ability to learn and anticipate change then maintaining BCM will be a difficult process.

Hiles (2007c) advocates that BCM practitioners do not use a 'big stick' approach when raising awareness of BCM as this can backfire. As noted by Aronson (1999), there are two possible reasons why people conform. Either because the behaviour of others convinces them to conform or that they want to avoid punishment 'the stick'. People respond better to persuasion rather than by being threatened. Considering why individuals conform further, Aronson (1999) says that to get the required response from an individual they must internalize the value or belief as this is the most permanent way of getting the most deep rooted response. This holds true for a BCM programme which must be internalized by all in the organization in order to be successful. Compliance is less enduring and has less effect on the individual than internalization according to Aranson (1999). Hiles (2007c) recommends getting a statement of support from the CEO or the board on the importance of the BCM programme to ensure its effective implementation.

The two main elements that need to be present in order for a BCM process to be successful in an organization according to Elliott, Swartz and Herbane (2010) are, firstly the organization structure needs to be in place to ensure clear communication lines of authority, control and communication and secondly organizational conditions need to be correct for effective implementation of the BCM.

A word of warning regarding the effects of a dysfunctional organizational culture and cognitive dissonance is sounded by Kotnour (2009):

> "We can have our values in books, cards that we give to everyone, on plaques on the wall, but if we don't have those values in our hearts and in our behaviour, we have a dysfunctional culture. In essence, it's dissonance. Cognitive dissonance occurs when our thoughts (cognitions) and our actions are opposed to each other. In engineering terms, we have a state of disequilibrium. In practical terms, something's gotta give. What usually "gives" is the values change to match the dysfunctional culture among a small set of individuals." (Kotnour 2009, p. 1)

Embedding BCM into the organizational culture therefore requires an awareness of the wider existing organizational culture and must be undertaken carefully in order for it to become internalized by employees for the future. Having all of the above BCM programme elements in place should lead to the organizations BCM programme being comprehensive and functional from its inception and throughout the lifetime of the organization.

2.3.1.7 BCM and Change Management

It is vital that BC plans are constantly maintained, Gallagher (2003) warns that if BC plans are not kept up to date following organizational changes they will become irrelevant. Elliott, Swartz and Herbane (2002) make reference to the fact that more attention has often been directed to the planning dimension of the BCM process than that of implementation, both in practice and in various publications. Kjærgaard (2009) outlines that when it comes to organizational change and maintaining BCP's, organizations face a dilemma when they engage in strategy-making, because they must reconcile the constant tension between continuity and change. As organizations face constant change as a result of today's business environment, the BCM management strategy needs to be flexible enough to be able to keep pace with this challenge.

The literature notes that it is important that in any BCM process plans are kept updated as the organization evolves over time through a change management (CM) process. The BCM programme therefore needs to be part of the organizational CM programme in order for it to be kept current. Armit (2007) refers to this noting that plans reflect the business requirements at that time. Requirements and recovery times are not constant and must be maintained via a BCM, CM process. Commenting on the CM of the BC programme, Elliott, Swartz and Herbane (2010) state that generic change management strategies should be used to ensure effective BCM implementation.

Looking specifically at organizational change in more detail Johnson and Scholes (2002) identify four types of strategic change, adaption, reconstruction, evolution and incremental.

According to Johnson and Scholes (2002), whichever change management style is adopted for the BCM process it can be managed in one of five ways, education and communication, collaboration, intervention, direction, coercion.

When the business continuity CM process is being put in place it should be a part of the wider organizational CM process used within the organization.

With regard to the BCM programme implementation, The Standard advocates that the organization needs to communicate the programme to stakeholders; arrange or provide appropriate training for staff; and exercise the business continuity capability.

Once the BCM programme has been included in the organization CM process maintaining it will fall into line with the maintenance of other processes. Gallagher (2003) advocates keeping the groups used to create the BC plan together. They may meet less frequently, but they provide a focus for the work at an operational level and also help to ensure the effective communication of business continuity issues between different departments or units

In order for a BCM programme to be successful a prerequisite is that the organization is understood at multiple levels.

2.3.2 Understanding the Organization

As evidenced from the literature, the foundation underpinning effective BCM involves gaining a deep understanding of the organization and all its constituent parts including external entities and the environments within which it operates. As referred to in The Standard the main aim of this element of the BCM programme is to help in understanding the organization by identifying its main products and services and the resources and activities that support them. This process aligns the BCM programme with the organizations objectives.

Understanding an entire organization can be a daunting undertaking for the BC professional and requires a knowledge of multiple areas of the business.

Understanding, in the sense of BCM, is described by Rossing (2007) as having a thorough knowledge of mission-critical activities and their relationship to the organization as a going concern.

Sheth, McHugh and Jones (2008) diagrammatically represent the multiple external links that organizations are often subject to and also the multiple and disparate bodies, people and organizations that go to make up the environment in which an organization operates.

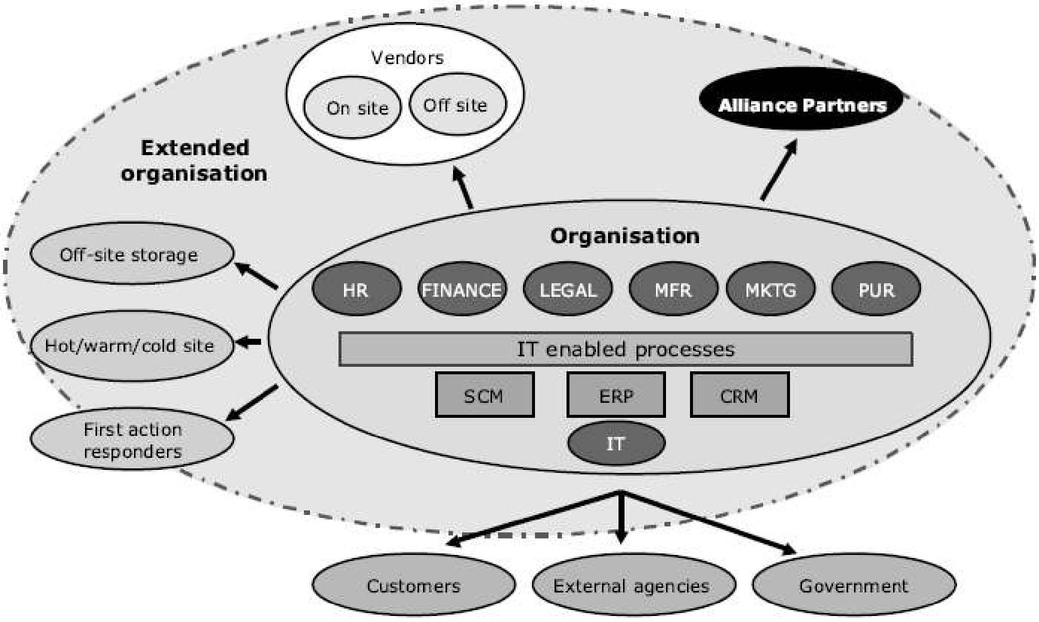


Figure 2.4: The extended organisation
(Sheth, McHugh and Jones 2008, Figure 3, p. 226)

BCM literature has a significant focus on the continuity of supply chains and their impact on organizations. Sheffi (2007) outlines the importance of protecting the wider organizational supply chain, recognising that while modern supply chains give high levels of customer service and low costs they are also vulnerable to high-impact/low-probability events. Noting the importance of supply chains to not only organizations but also governments, the World Economic Forum (2008) identifies that all companies and governments dependent on external suppliers are exposed to the risks of disruption in their supply chain. The extent and complexity of current global supply chains mean that the problem of supply chain management is not limited to a single enterprise or industry: even a relatively small supply chain disruption caused by a global risk event may ultimately have consequences across the global economic system.

Organizations face a dilemma notes Perrow, as cited in Smith (2005). They need to behave as rational entities that are systematic, work through well-defined and tested "rules for action" and are both open and transparent in their decision making processes. On the other hand, they need to interact with a wider world and this creates problems for control and containment. Organizations are therefore in a constantly state of flux between openness and control and between rational behaviour and vested self-interest according to Perrow, as cited in Smith (2005). These tensions, along with the difficulties of making sense of the prevailing conditions and predicting their future outcomes, virtually guarantee that the potential for crisis is incubated.

2.3.2.1 Dealing with Unknown Events

Dealing with unknown events or being prepared in some way for the unknown is highlighted throughout the BCM literature. Unknown events by their very nature present organizations with some of the biggest challenges when implementing a BCM programme. Elliott, Swartz and Herbane (2010) say that business continuity practitioners and managers need to think creatively about potential interruption scenarios and their possible impacts upon activities and stakeholders. They recommend adopting a creative, multi-perspective, iterative and questioning mind-set. With regard to crisis events (unknown events), Lagadec (2009) submits that the problem is no longer to identify what we "still" do not know, but more modestly to try to discern what parcel of our available knowledge really is robust enough to answer the surge of questioning from all sides that modern crises elicit, and to guide us through them when all else fails.

Considering unknown events further, Taleb (2007) refers to a single observation (a Black Swan event) invalidating a general idea that has held true for millennia. Black Swan events have three attributes according to Taleb (2007), they lie outside what is regularly expected, they carry an extreme impact and finally human nature allows us to concoct explanations for these event occurrences after the fact, allowing us to explain the event away in a logical manner. Black Swan events are summarized by Taleb (2007) as having rarity, extreme impact, and retrospective (although not prospective) predictability. He highlights that we need to acknowledge that the unexpected can occur. These unexpected events are generally what drive history. Wars, pandemics and stock market crashes appear predictable with the benefit of hindsight. At the time, however, such occurrences generally come as a major shock.

In a similar vein to Taleb, Youngblood (2000) states, using examples from evolution, that seismic quantum shifts or as scientists call them 'punctuated equilibria' occur as illustrated in Figure 2.5. Stable environments are subject to periodic tremendous churn effecting all within the environment and this equally applies to organizations.

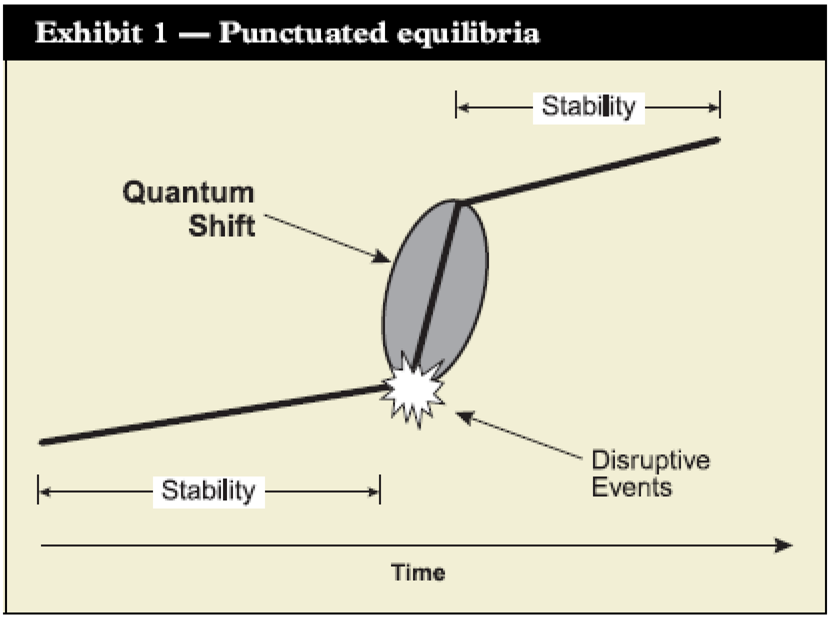


Figure 2.5: Punctuated equilibria
(Youngblood 2000, Exhibit 1, p. 5)

Referring to rare/extreme events, Alesi (2008) further notes that business continuity planning is in a constant state of change and development. Changes can be slow and almost imperceptible, but may also be rapid having far-reaching consequences. When change occurs suddenly, it is often accompanied by an unforeseen, external event and can have multiple impacts on the organization.

Having an understanding of these rare event occurrences, an ability to predict their effects upon an organization and having a flexible and modular BC plan can enable a fuller and better functioning BCM process which can effectively cope with the rare and extreme impact event. Part of the ability to deal with unknown events will be to conduct a business impact analysis in order to fully understand the organization and the impact of crisis upon it.

2.3.2.2 Business Impact Analysis (BIA)

The main technique used to gain a greater understanding of an organization and its process according to the literature is the Business Impact Analysis (BIA). Elliott, Swartz and Herbane (2010) note that the BIA forms the backbone of the entire BCM process and that the BIA means having to assess the likely financial and operational consequences of a crisis. The BIA helps to identify the critical processes, priorities and single points of failure alongside the key dependencies both internal and external and any inherent risks and vulnerabilities that may exist within an organization according to Smith and Shields (2007).

The Standard recommends that for each business activity which supports the delivery of critical products and services the organization should assess the impacts of disruption on activities over time, determine the maximum tolerable disruption period for each activity and identify any interdependent activities.

As a result of the BIA, BCM practitioners can therefore determine each business function's recovery time objectives (RTO). RTO is defined by Barnes (2001) as the amount of time allowed for the recovery of a business function. If the RTO is exceeded then severe damage to the organization would result.

The BIA process will also give an insight into the recover point objective (RPO). RPO according to Bradbury (2008) determines from what point in the processing cycle is the data going to be recovered? In other words how much data is the organization prepared to lose or have to re-enter. Finally the BIA enables an assessment of the maximum tolerable period of disruption (MTPD). The MTPD as defined by Bradbury (2008) as the maximum time that a business will survive from the initial service interruption.

All of the above measures give the BCM practitioner a clearer view of the wider business and its recovery requirements. It is important to note that the business requirements determine the overall recovery objectives. As outlined by Bradbury (2008), any recovery objectives must be based upon solid business requirements which are identified by the BIA process. He diagrammatically shows the BIA process and the correlation between the incident starting time, the incident reporting process, the incident investigation process, the decision making process, and the recovery process alongside the RTO.

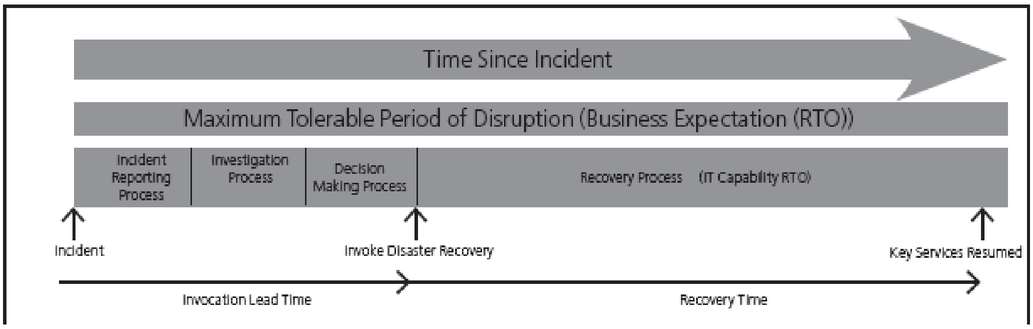


Figure 2.6: The Business Impact Analysis Process
(Bradbury 2008, Figure 1, p. 14)

Having these time estimates and also any associated costs incurred from the disruption lets management decide where their often scarce recovery funds and resources are allocated. Taking a more cost conscious approach to the BIA, Myers (2006) suggests that in order to keep the costs of BCM at acceptable levels when running a BIA that it is important to let others know the context (i.e. that the mind-set is survival rather than business as usual) in which the BCM questions are being asked. The purpose of the BIA according to Myers (2006) is not to document potential loss so that management will make contingency planning a high priority, nor is its purpose to cost-justify redundant processing capability. The BIA, as noted by Myers (2006), should make managers comfortable in taking part in the BCM process, educate managers in the costs associated with various solutions and help to evaluate all the options.

Looking further at the literature regarding BIA, Gallagher (2003) says that the BIA is an exercise in homing in on the things that are important rather than the ‘hobby-horses’ of particular managers.

Elliott, Swartz and Herbane (2010) point out that the BIA also offers an analysis of some of the idiosyncrasies of the organizations resources, systems and operations.

To ensure a complete and comprehensive, cost efficient BCM process it is vital a thorough BIA is undertaken in order to provide an understanding of the overall organization and its recovery requirements.

2.3.2.3 Identification of Critical Activities

Once the BAI is completed this allows an analysis of the organizations activities to take place to ascertain which are crucial and what needs to be undertaken in order to recover them. As suggested by Elliott, Swartz and Herbane (2010), the next process to be undertaken is to build on the BIA through a systematic analysis of the organization’s operating environment and a detailed examination of its outputs, activities and dependencies. In order to determine what is critical Myers (2006) maintains that when the question “what is critical” is asked, it is to discover which technology should be given restoration priority following a disaster. This analysis should also extend to all areas of the organization. The Standard outlines that an organization may want to focus its planning activities on critical activities, but should recognize that other activities will also need to be recovered within their MTPD.

The importance of keeping the BIA and other elements of the BCM programme updated cannot be over emphasised. Koch (2004) highlights that without an iterative BIA, recovery plan and technical review process ultimately the BC programme will fail and become out-dated.

2.3.2.4 Determining Continuity Requirements

Upon completion of the BIA the main organizational continuity requirements will have been identified and the next requirement according to the literature is to estimate the resources that each activity will require in order to resume. The resources required may include some if not all of the following: people; knowledge; skills; premises; supporting technology; plant; equipment; information (electronic or paper based); and 3rd party or external resources such as network providers. The needs of the wider external stakeholder community should also be considered. Elliott, Swartz and Herbane (2010) recognise the importance of acknowledging the impact of external stakeholders as part of their crisis management approach to BCM.

One of the issues at this stage of the BCM process is over/under estimating the requirements that are needed to keep the critical business functions running. Barnes (2007) recognises that there is sometimes a tendency for those assessing requirements to assume that business continuity means the creation of an environment for continuation of business as usual. This may indeed be the intention in a small minority of cases, but in the majority of cases what is sought, at least initially is that the organization can continue what is critical using a minimalist approach. Barnes (2001) notes that ultimately it is up to the CEO or senior management to decide what is/is not included under the BCM process.

2.3.2.5 Evaluating Threats to Critical Activities

A crucial element of any BCM process according to the literature is the need to undertake a risk assessment. This is where the lines between BCM and Risk Management (RM) or Risk Assessment (RA) may appear to blur as they are essentially looking at the same threats. As noted by Vaid (2008), no discussion on BCM can be complete without reference to operational risk

RA is defined by Elliott, Swartz and Herbane (2010) as the term used to describe the process of gauging the most likely outcomes of a set of events and the consequences of those outcomes.

Whittet (2008) notes that operational risk is defined in Basel II as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. When addressing the key elements that comprise RM/RA, O'Hehir (2007) mentions that they are the risk appetite of the senior management/board, analysis of internal and external risks, controls to mitigate risks and a risk monitoring process to ensure the RM system works.

To help in evaluating the risks to an organization, Charters (2007) advocates seeking advice from insurers, local trade associations or business continuity user forums to assess the likelihood of specific threats in the location in which the organization operates and suggests that a structured approach to risk evaluation which consists of four main steps: asset and threat identification, quantification of potential losses, assessment of vulnerabilities and evaluation of solutions.

The vulnerability of an organization to a disruptive event according to Sheffi (2007) is made up of a combination of the likelihood of the disruption and its potential severity. It is highly unlikely that a business can remove all risks entirely as some level of risk is inherent in all activity, but as noted by Charters (2007), by concentrating on just the core business, this can lead an organization to miss other risks that have not been identified. The core business risks have to be addressed as a priority by the organization and as alluded to by Gallagher (2003), the risks must be subject to a realistic evaluation and management but this does not mean that non-core risks should not be addressed. When considering small risks that may not seem to have a bearing on an organization the BCM practitioner should be aware that small disturbances can rapidly spread due to the interconnection between organizations. As noted by Perrow (1999) as cited in Boin (2009):

> "in our just-in-time societies, small disturbances propagate rapidly through the dense networks that connect them…. Modernization has created 'highways for failure' that leverage the effects of emerging threats (be they man-made or natural)." (Boin, 2009, p. 370)

When evaluating threats an important point to note is that most incidents faced by organizations are minor or certainly in the majority of cases not full disasters. Ginn (1992) alludes to this outlining, that although the BC plan is designed to cope with a total disaster, the worst-case situation, in many cases the disasters which occur will be minor or intermediate in nature. Commenting further on operational risks, Whittet (2008) says that risks can be further broken down into seven general categories, internal fraud, external fraud, employment practices and workplace safety, clients, products and business practice, damage to physical assets, business disruption and systems failures, execution, delivery and process management.

It should be borne in mind that identifying all of the most likely event outcomes and consequences can be problematic or extremely difficult in the case of complex systems and Elliott, Swartz and Herbane (2010) note that any attempt to quantify risk will fail because, no matter how sophisticated the mathematics are, all risk assessment is inherently value laden.

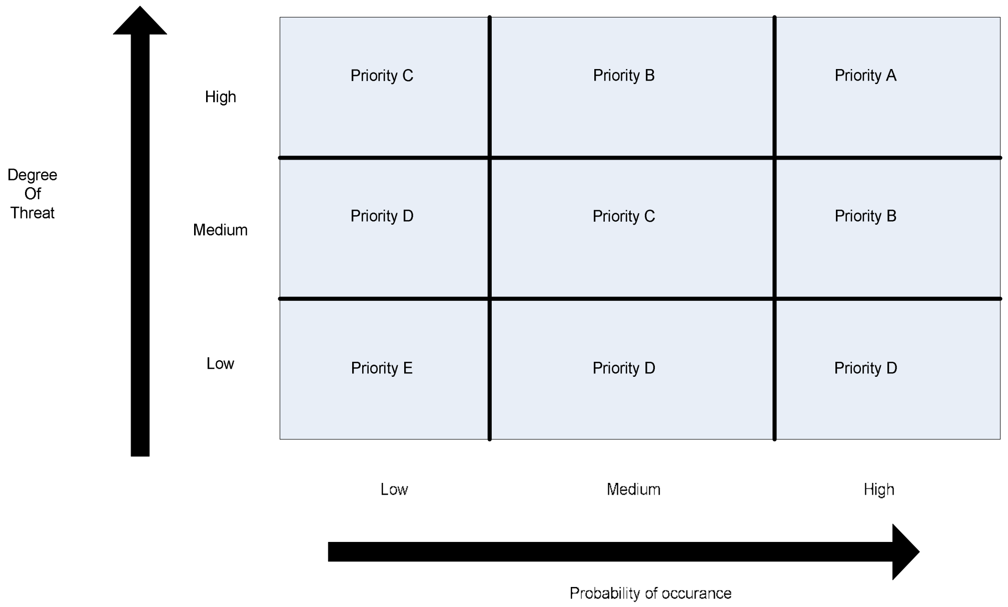
2.3.2.6 Methods of Risk Assessment

BCM is also closely aligned with other management processes such as operational risk management. The objectives of operational risk management as outlined by Viner (2007) are to identify, assess and control risks so that the business will not be prevented from achieving its objectives. In order to assess risk various types of risk matrices are suggested in the literature reviewed to help an organization assess the impact of risks identified in the BIA and to prioritise remedial actions. A couple of these are outlined below and discussed briefly.

Impact Probability	LOW	HIGH
HIGH	Manage	Reduce
LOW	Accept	BCP (Plan)

Figure 2.7: Risk and impact matrix,
(Charters 2007, Figure 10.1, p. 142)

When using the Charters (2007) matrix, if the probability of the risk is low and the impact is low, then the risk is acceptable, if the probability is high and the impact is low, then the risk should be managed etc.



	Low	Medium	High
High	Priority C	Priority B	Priority A
Medium	Priority D	Priority C	Priority B
Low	Priority E	Priority D	Priority D

Figure 2.8: Risk Assessment matrix.
(Elliott, Swartz and Herbane 2010, Figure 5.10, p. 165)

The risk assessment matrix as outlined above (Figure 2.8) uses a risk priority method which depends on the likely probability of occurrence of the risk and the degree of threat posed by the risk. Depending on whether the chance of the risk occurring is low, medium or high it will then be assigned a priority. Priority A risks, are those that are most likely to occur and have the highest probability of occurrence.

These risk matrices approach the problem from slightly different perspectives e.g. impacts versus degree of threat but will all result in the organizations risks being assessed.

It should be noted that according to Sheffi (2007), high-probability/low-impact events are part of everyday operations, whereas low-probability/high-impact events call for planning and are outside the realm of daily operations. Sheffi (2007) provides an example of a concentric vulnerability map that is used by

General Motors (GM), this is another tool that helps categorises disruptions that the organization could face and may be a useful tool for organizations to adopt.

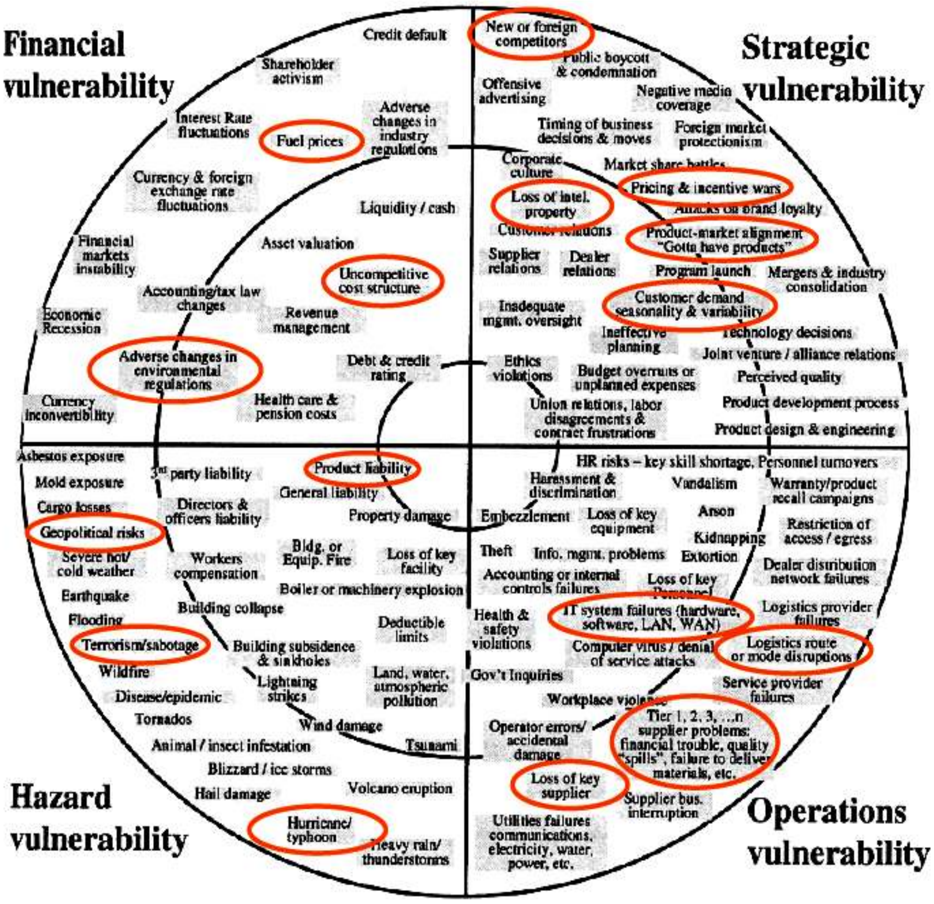

Financial vulnerability
Strategic vulnerability
Hazard vulnerability
Operations vulnerability
Credit default
Shareholder activism
Interest Rate fluctuations
Fuel prices
Adverse changes in industry regulations
Currency & foreign exchange rate fluctuations
Liquidity / cash
Financial markets instability
Asset valuation
Uncompetitive cost structure
Accounting/tax law changes
Economic Recession
Revenue management
Adverse changes in environmental regulations
Debt & credit rating
Currency inconvertibility
Health care & pension costs
New or foreign competitors
Public boycott & condemnation
Offensive advertising
Negative media coverage
Timing of business decisions & moves
Foreign market protectionism
Corporate culture
Market share battles
Pricing & incentive wars
Loss of intel. property
Attacks on brand loyalty
Customer relations
Product-market alignment "Gotta have products"
Supplier relations
Dealer relations
Program launch
Mergers & industry consolidation
Inadequate mgmt. oversight
Customer demand seasonality & variability
Ineffective planning
Technology decisions
Joint venture / alliance relations
Ethics violations
Budget overruns or unplanned expenses
Perceived quality
Union relations, labor disagreements & contract frustrations
Product development process
Product design & engineering
Asbestos exposure
3rd party liability
Product liability
Mold exposure
General liability
Cargo losses
Directors & officers liability
Property damage
Geopolitical risks
Severe hot/ cold weather
Workers compensation
Bldg. or Equip. Fire
Loss of key facility
Earthquake
Boiler or machinery explosion
Building collapse
Flooding
Deductible limits
Terrorism/sabotage
Building subsidence & sinkholes
Wildfire
Lightning strikes
Land, water, atmospheric pollution
Disease/epidemic
Tornados
Wind damage
Animal / insect infestation
Tsunami
Blizzard / ice storms
Hail damage
Volcano eruption
Hurricane/ typhoon
Heavy rain/ thunderstorms
HR risks – key skill shortage, Personnel turnovers
Harassment & discrimination
Vandalism
Warranty/product recall campaigns
Embezzlement
Loss of key equipment
Arson
Restriction of access / egress
Kidnapping
Theft
Info. mgmt. problems
Extortion
Dealer distribution network failures
Accounting or internal controls failures
Loss of key Personnel
Logistics provider failures
Health & safety violations
IT system failures (hardware, software, LAN, WAN)
Computer virus / denial of service attacks
Logistics route or mode disruptions
Gov't Inquiries
Service provider failures
Workplace violence
Operator errors/ accidental damage
Tier 1, 2, 3, …n supplier problems: financial trouble, quality "spills", failure to deliver materials, etc.
Loss of key supplier
Supplier bus. interruption
Utilities failures communications, electricity, water, power, etc.

Figure 2.9: Concentric Vulnerability Map

(Sheffi 2007, Figure 2.3, p. 25)

Vulnerabilities listed towards the centre of the vulnerability map tend to come from within the organization where as those listed at the periphery tend to come from outside. Another tool that can be used to prioritise possible organization vulnerabilities is the Enterprise Vulnerability Map (EVM). Sheffi (2007) recommends using an EVM to give a graphic representation to help managers visualise their organizations vulnerabilities and how they may impact

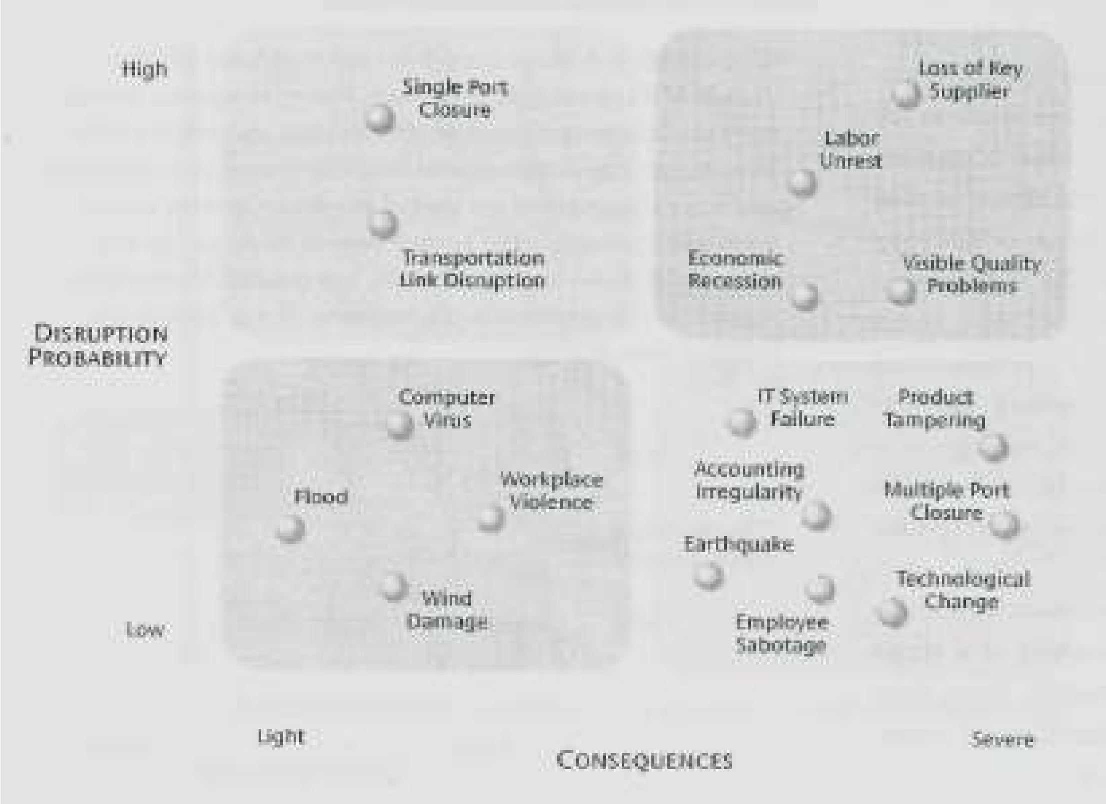


Figure 2.10: Enterprise Vulnerability Map,
(Sheffi 2007, Figure 2.4, p. 32)

The EVM (which is similar to previously outlined risk matrixes) measures risks to the organization against the likely consequences of the risk and the likely probability of the disruption occurring.

Once the known risks have been assessed it is then that the rare events can be addressed. This is not an easy exercise as human nature (dealing with uncertainty) does not lend itself easily to this task.

2.3.2.7 Predicting Rare Events

Throughout the BCM literature reviewed, the theme of dealing with rare events occurs. As pointed out by Taleb (2007), predicting rare events is not an easy exercise as by their very nature it is often impossible to imagine or predict all eventual outcomes. Expanding further Taleb (2007) notes that the human condition makes us focus more easily on what is normal at the expense of ignoring the more infrequent events that contain large amounts of uncertainty.

When rare events occur we have to deal with uncertainty according to Taleb (2007). He argues that:

> "Almost everything in social life is produced by rare but consequential shocks or jumps; all the while almost everything studied about social life focuses on the "normal," particularly with "bell curve" methods of inference that tell you close to nothing". Why? Because the bell curve ignores large deviations, cannot handle them, yet makes us confident we have tamed uncertainty." (Taleb 2007, p. xxiv)

Alluding further to difficulties in predicting rare events, Charters (2007) highlights some of the difficulties in assessing specific threats due to the fact that certain threats are more prevalent in particular locations, earthquakes can cause damage many miles from their point of origin, most IT failures are user generated, internal threats are more likely to occur than external, flooding does not necessarily occur on the lower floors (e.g. where water tanks are installed on the roof) etc. However despite the preceding concerns Elliott, Swartz and Herbane (2010) advocate that using a structured approach to risk assessment is better than not using one at all.

Standard risk assessment frameworks such as BS ISO/IEC 27001 can be adopted in order to help assess rare events or indeed any risk. Typical constituents of such a framework are that they set out the criteria for risk acceptance, identify what are acceptable levels of risk for the organization and performance of an analysis of the risks.

An on-going risk assessment and management programme is also vital as risks come and go due to the changing environment in which most organizations operate. Recent years have provided us with many examples of the kind of changing risk profile organizations face with the occurrence of the flu pandemic, the Icelandic Eyjafjallajokull volcano and its disruption to transport and the harshest winter in 28 years all being experienced.

2.3.2.8 Determining Choices.

According to the literature, once the risk assessment process has been undertaken and the risks identified, categorized and prioritized in conjunction with the BIA, it is then that the attention shifts to the process of mitigating, accepting or ignoring the various risks that have been presented.

The Standard alludes to the fact that these risk mitigation measures are sometimes referred to as the ‘4 T’s’ model. Treat the risk in order to lessen its impact, Tolerate, i.e. accept the risk, Transfer (e.g. insure against the risk) or Terminate (get rid of the risk). Charters (2007) and The Standard both mention that when looking at solutions, risk control measures fall into five categories: accepting the risk, managing the risk, transferring the risk, change suspend or terminate the risk and plan for the risk.

The Standard states that for each risk, measures to reduce the likelihood of a disruption, lessen the period of disruption, and lower the impact of a disruption on the key organizational products and services should be implemented. The measures to accomplish these tasks are often referred to as loss mitigation, risk treatment or risk control. This is alluded to by Elliott, Swartz and Herbane (2010) who note that the BIA, re-evaluates the initial BCP objectives and assesses the risks against those objectives. Thus the BIA should incorporate an assessment of the resources that each business unit and function require to resume at an appropriate time. Such an analysis can provide multiple alternative resumption scenarios. Elliott, Swartz and Herbane (2010) refer to this stage of the BCM process as the Business Impact Evaluation (BIE) and outline that the BIE is made up of four analyses:

1. Business continuity objectives are refined.
2. Risks are evaluated.
3. Priorities for business recovery are established.
4. Business interruption scenarios are developed.

2.3.2.9 Sign Off

Senior management should as is the case with the other BCM stages, sign off the various documents that have been created so far as part of the BCM process to ensure that the work has been appropriate and is a true reflection of the organization. The document set includes the documented list of key products and services, the BIA and BIE and the risk assessment documentation.

2.3.3 Determining Business Continuity Strategy

As a result of the BIA and the subsequent analysis, an organization will be better placed to choose an appropriate continuity strategy to enable it to meet its strategic objectives. In the context of BCM, strategy concerns the determination and selection of alternative operating methods to be used to maintain or restore the organization's key products and services and their supporting critical activities after an incident, to an acceptable minimum level. As noted by Johnson and Scholes (2002), strategic decisions are about trying to achieve some advantage over your competitors and strategy can be seen as the matching of the resources and activities of an organization to the environment in which it operates. The BCM strategy an organization selects could therefore help it gain a competitive advantage over its rivals.

Culture and politics play an important role in strategy selection, according to Johnson and Scholes (2002) and they outline the phases of strategy decision making as being, issue awareness, issue formulation, solution development and the selection of solutions.

When selecting an appropriate BCM strategy for a product or service the literature recommends using the documentation already created as part of the BCM process particularly the BIA and to be aware of the RTO, RPO and MTPD of the organizations key services/activities.

2.3.3.1 Strategy Options

All organizations need to consider the strategic options available for their critical activities and the resources required in order to resume those activities. Whatever strategy is chosen Courtney (2007) points out that it must be complete and meet all recovery requirements without any gaps or weakness. Further factors to be considered when selecting an appropriate recovery strategy are according to BSI (2006), the MTPD, the costs of the implementation or strategy and the impacts of doing nothing. Commenting further on strategy, Barnes (2001) says those responsible for BCM must weigh the cost of being without the service at various points in time (the duration of the outage) against the cost of the solution. The objective here is to minimise the cost of the impact and the solution.

Several alternate strategies should be considered where possible. Courtney (2007) points out that these alternative strategies (he recommends choosing at least three alternate strategies) should provide a range of recovery times and certainty of recovery at different cost levels. A risk analysis of each strategy should be performed before the different strategy options are presented to senior management. The Standard suggests that a separate strategy may be required for the following resources, people, premises, technology, information, supplies, stakeholders and civil emergencies. Barnes (2001) outlines in graphic form the recovery times required by various recovery options. This is of interest as it shows that the more real-time an organizations recovery strategy, the higher the cost of that strategy is likely to be.

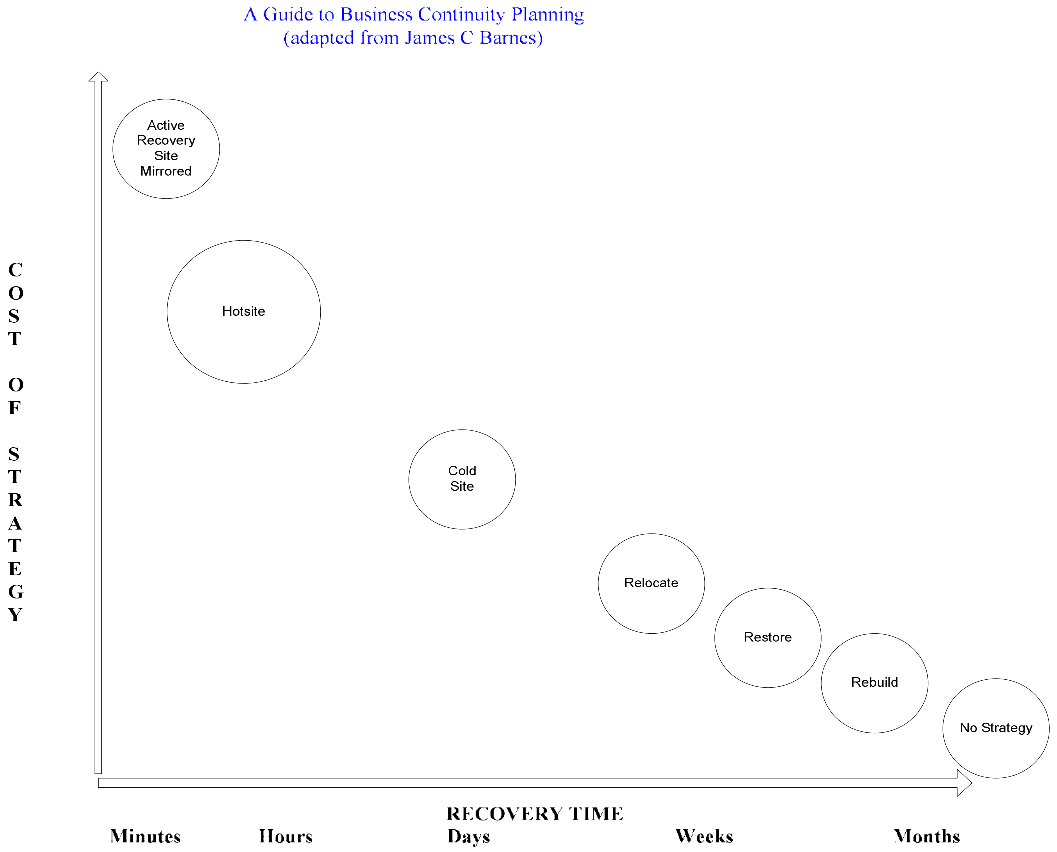


Figure 2.11: IT strategies that are available and RTO they must satisfy (Barnes 2001, Figure 4.3, p. 93)

When choosing a business continuity strategy an organization should select one that reflects the recovery requirements within the corporate policies of the organization. Courtney (2007) advocates selecting the most cost-effective solution. Any chosen strategy will most likely be a balance between cost and peace of mind.

2.3.3.2 People

Reviewing the available literature regarding the BCM strategies for people, it is recommended that the organization should identify appropriate strategies to maintain core skills and business knowledge. The analysis should not only include employees but should also include contractors and other stakeholders who may possess specialist skills and knowledge that are required by the organization. The Standard identifies a number of strategies that can be used to protect or provide these skills including ensuring that all critical activities of an organization are well documented and the more staff that have multiple skills the more resilient the organization is likely to be. Strategies for skills separation and covering skills across multiple staff resources or by using third parties will also aid in recovery of the organization from a crisis event. Looking at succession planning in particular, Perman (2009) states that, organizations can experience large financial losses when they are unprepared for a key employee's departure. Delays in finding a replacement are also often common. Perman (2009) further maintains that during extended periods of vacancies, projects can be delayed, revenues may be unrealised, customers lost, innovation can often stop or slow, overtime costs may rise and employee morale often drops. The main benefits of a successful succession planning process are according to Perman (2009) that it, smooth’s job transitions; gives job assignments that properly prepare candidates for their new positions; ensures meaningful appraisals and feedback; ensures appropriate selection criteria and results in having cover for key roles. Succession planning can take various forms e.g. job-rotation within and outside departments and divisions, job shadowing and job sharing can also be used where two individuals provide cover for each other’s roles and therefore become multi-skilled and so limit the risks associated with only one employee having all the key knowledge.

All of the above possible impacts need to be considered when looking at people strategies during a BCM programme. It should also be borne in mind that in times of crisis even the most robust employees may be rendered incapable due to traumatic events. Gallagher (2003) notes that until recently, many plans have virtually ignored the fact that a disaster could result in significant loss of life with all its associated human and psychological impacts. It is therefore advisable that human resources ensure that the organization has the best possible BC personnel strategies in place.

2.3.3.3 Premises

The literature notes that the organization should devise a strategy for reducing the impact of the unavailability of its normal worksite(s). The Standard suggests this may include one or more of the following options: alternative premises within the organization, alternative premises provide by other organizations, alternative premises provided by third-party specialists, working from home or at remote sites, other agreed suitable premises and use of an alternative workforce in an established site.

2.3.3.4 Technology

Choosing an appropriate technology strategy according to the literature, will depend on the nature of the technology employed and its relationship to critical activities.

As pointed out by Jackson (2000), there is rapid development in the area of technology with systems and tools rapidly changing over time, organizations must adapt their processes to keep up with these advances. Sometimes, those that are not prepared for these issues find themselves with a patchwork of technologies that create areas of weakness and possibilities for failure.

Some technology strategies that can be used according to the literature are, maintaining multiple IT locations, using older equipment as emergency replacement or spares, additional risk mitigation for unique or long lead time equipment and having standby equipment ready or a reciprocal arrangement with someone else. IT services often require complex continuity strategies. When selecting these strategies consideration should also be given to the RTO for systems and applications which support the critical BIA activities, the number and location of and distance between technology sites, remote access options, redundant telecommunications routing, the nature of the failover (whether its automatic or needs manual intervention), 3rd party connectivity and external links and the use of unstaffed technology sites. Other items that can be added to this list are the provision of backup generators to provide power in the event of failure and also the provisioning of uninterrupted power supplies (UPS's) to take up the power load whilst generators come on-line.

All of these strategies come with associated costs and complexity and it is up to the BCM coordinator to assess the merits of each strategy before selecting one or more to present to senior management. The complexity of IT recovery strategies is further complicated today by the growth in the amount of data that organizations use. As identified by Preimesberger (2009) and Chen (2007), the growth in data that companies, governments and other users now store presents a further BCM challenge. Chen (2007) refers to this challenge as 'digital preservation'. This extra data will need to be stored and protected by BCM systems adding cost and complication and represents a serious challenge to organizations. Preimesberger (2009) identifies that the swift data growth and subsequent need for storage is due to the likes of high-resolution video, surveillance video, high-end video games, and high-resolution photos and graphics data being used by organizations today and also recognises that business continuity technologies are improving almost daily, through the increasing use of virtualization, de-duplication and thin-provisioning methods which allow an organization to keep only important data. According to Chen (2007) the fact that hardware and software are subject to upgrades on a frequent basis can also lead to data retrieval issues as old storage technologies become out-dated.

Although IT organizations generally have enough funding to support their on-going IT operations, they often run short of funding when it comes to buying secondary infrastructure required to deploy a robust business continuity response according to Vizard (2008). Commenting further on this issue Vizard (2008) puts forward the view that this is primarily due to the fact that the vendor community has always viewed business continuity as an opportunity to sell additional products and advocates that the underlying IT infrastructure should be intelligent enough to provide an embedded business continuity capability. Vizard's notes that the best answer to this conundrum would be for every product to simply plug into a fabric in which every device automatically supports every other system.

While most IT departments and IT vendors are a long way from Vizard's vision it is however a goal worth striving for in terms of the purchase, maintenance and installation costs of IT infrastructure and would lead to far clearer and less complicated IT recovery strategies. This is perhaps one area in which current cloud computing initiatives can benefit BCM by removing the need for organizations to maintain their own IT infrastructure and instead use a cloud based purpose built infrastructure managed by an expert supplier. Recent outages of Amazon and Microsoft's cloud based services have however brought the resiliency of the current cloud services into question.

2.3.3.5 Information

Information recovery strategies are required to ensure that information vital to the organization's operation is protected and recoverable according to the timeframes described within the BIA. Any information required for enabling the delivery of the organization's critical activities should have appropriate, confidentiality; integrity; availability; and currency.

Gallagher (2003) says that despite the organizational dependence on IT systems, databases and e-mail facilities, paper files still provide vital records for most organizations. The importance of this paper based source must be taken into consideration when developing business continuity strategies as they can be often overlooked. The most obvious areas are the legal and contract realms where electronic copies of the signed documents may not be available or acceptable. Other areas such as finance and human resources may also have significant paper records that need to be considered.

Backup strategies for information need to be robust and tested on a regular basis to ensure that should a crisis occur they are adequate and provide the organization with the required contingency levels. Backup strategies include both technological (tape and disc backups) alongside offsite storage of vital documents to specialist providers or alternate organizational backup facilities. Information strategies should also be documented for the recovery of information that has not yet been copied or backed-up to a safe location.

2.3.3.6 Supplies

The BCM literature outlines that organizations should identify and maintain an inventory of the core supplies that support its critical activities. Strategies to provide on-going supplies according to The Standard, may include, storing additional supplies at other locations, having third parties who deliver stock at short notice, split just-in-time deliveries to other locations, holding materials at warehouses or shipping sites, identification of alternative/substitute supplies. Where critical activities are dependent upon specialist supplies the organization should identify the key suppliers and unique or single sources of supply which may represent a single point of failure. Strategies used here to manage continuity of supply may include, having multiple suppliers of certain components; ensuring or requiring suppliers have a validated business continuity capability, SLA's with key suppliers or the identification of alternate suppliers.

The supply difficulties that can occur typically result in greater delivery times, differences in supply quality, relationships with customers becoming strained, customers replacing their usual supplies with other brands and rival organizations boosting their sales, according to Gallagher (2003).

2.3.3.7 Stakeholders

It is evident from the literature that an organization has a responsibility to all its stakeholders in times of crisis. This includes both internal and external stakeholders. As far back as 1976, Turner recognised that the brief of business continuity had been widened to take into account the fact that crisis incidents contained both social and technical elements. BCM has therefore to take into account not only the technical side but also the human, organizational and social aspects of the organizations environment and is seen as a unifying process.

The Standard notes that when devising appropriate BCM strategies, the organization should consider, manage and protect the interests of its key stakeholders. Strategies to protect the interests of key stakeholders may include special arrangements for those stakeholders with specific needs, such as employees with particular requirements due to disability, illness or pregnancy. As with selecting any strategy the wider supply chain needs to be considered in the BCM process as members of the supply chain are stakeholders in the organization both up and down the chain. Oldfield (2008b) advises developing and maintaining supportive partnerships with critical stakeholders in the wider supply chain, sector and community and also advises consideration be given to which key stakeholders would support the organization in times of adversity, and which might attempt to undermine the organization.

The area of Corporate Social Responsibility (CSR) should also be considered. Zollo, Minoja, Casanova, Hockerts, Neergaard, Schneider and Tencati (2009) define CSR as a concept by which firms integrate the principles of social and environmental responsibility in their operations as well as in the way they interact with their stakeholders.

According to Zollo, Minoja, Casanova, Hockerts, Neergaard, Schneider and Tencati (2009) this definition shows that CSR can be viewed in two different ways, one from the interaction between the firm and its mainly external stakeholders and secondly from an internal change process which integrates CSR principles into the organization. As mentioned by Collicutt (2008), many organizations now consider corporate responsibility as a business differentiator and possible source of competitive advantage so it is crucial that it is included in BCM strategies.

One of the stakeholders often overlooked in BCM programmes are the actual employees. Gallagher (2003) alludes to this saying that most plans are based on the loss of assets and that people are often of secondary importance. This may be due to the fact that the origins of BCM are in disaster recovery (DR) a mainly technical focused discipline. The organization should identify a person or persons (normally within the human resources department) who discharge the responsibility for welfare issues following an incident.

2.3.3.8 Media

Organizations need to have a clear strategy for dealing with the media during a crisis as identified in the literature. Barnes (2001) recommends that only the CEO or dedicated staff with appropriate media training should be allowed to deal with the media. Gallagher (2003) also notes that it is vital in order to manage the media in the event of a disaster that every organization should have a clear, well understood and well-rehearsed media policy, media plan and media trained spokesperson. When dealing with the media there is an element of 'washing your dirty line in public' when announcing BC incidents. It is therefore vital that a concise and consistent message is given to the media from an organizations perspective.

2.3.3.9 Civil Emergencies

Civil emergencies are those emergencies that have an impact on the wider community and present a particular challenge to organizations due to the fact that the organization is no longer in control of the situation but is at the behest of the civil authorities and emergency services. Civil emergencies involve the likes of police and local authorities, so when forming BCM strategies for civil emergencies the organization needs to work closely with these external agencies to ensure it is included and aware of the wider plans. When devising any BCM strategy Gallagher (2003) notes that any plans have to include the emergency services as many BC plans finish at the factory gate. Often there is a gap in organizational BCM when it comes to the emergency services and these gaps cannot be ignored as this will lead to confusion over roles in the event of an emergency. Looking at the early stages of civil emergencies, Collicutt (2008) points out that local authorities, emergency services and other responders will be focused on saving life, limiting the spread of damage, and recovering essential utilities rather than on helping businesses.

In Ireland the Department of the Environment Heritage and Local Government (2006) published “A Framework for Major Emergency Management” which deals with civil emergencies. The document was designed to coordinate the actions of the Principal Response Agencies; therefore, it offers little or no advice to organizations on strategies for handling civil emergencies. It does however provide a view for the private sector as to how the public sector will deal with a civil emergency and how low down the priority list organizations appear to be for the civil authorities.

> “Private sector organizations may be involved in a major emergency situation in two ways.
>
> They may be involved through, for example, ownership of the site where the emergency has occurred or through ownership of some element involved in the emergency e.g. an aircraft, bus, factory, etc. They may also be called on to assist in the response to a major emergency by providing specialist services and equipment, which would not normally be held or available within the principal response agencies.”
> (A Framework for Major Emergency Management, 2006, pp. 76 –77)

It is therefore important that a strategy for dealing with civil emergencies is in place as part of the organizational BCM process. This should include making contact with the local authorities, Garda and Fire Officers in order to have lines of communication open during any emergency, to understand the role each plays during an emergency and also to share information with them as to what is contained in the organizations BCM strategy. Gallagher (2003) highlights the importance of including local public emergency services in any BCM strategy noting that there is an obvious need to work closely with the emergency services in preparing business continuity plans before a disaster actually happens. According to Gallagher (2003), it is necessary to understand their roles, procedures and practices in dealing with a disaster, and to know what input they could provide to make the organizational BCP more effective.

It is also important to consider the wider community when forming organizational BC plans. Organizations need to engage in developing community resilience for businesses according to Collicut (2008). Community resilience will help businesses to withstand the effects of a major regional or national emergency.

Collicut (2008) says there are three basic community groupings: local communities, functional communities and knowledge-based communities.

Somers and Svara (2009) recommend that local government should include the private sector in civil emergencies and that effective management of emergencies requires the non-traditional linking of agencies at different levels of government, as well as in the private sector.

Considering civil emergencies at a wider European level, Rhinard (2009) advocates wider international cooperation between nation states and notes that governments and public agencies will have difficulty in coping with crisis that have their origins outside their borders but have impacts within. Rinhard (2009) argues that European countries have become closely knit through technological innovation, economic integration, and political partnership. Common solutions including a single market, interconnected infrastructures, and systems for the free movement of people, goods, and services have been created. Whilst these solutions have generally brought prosperity and peace, they also hastened new problems. Multiple interstate interconnections generate interdependence and these interdependencies allow threats to move and escalate within a largely borderless European space. In 2008 the EU Council reached a political agreement on a directive on the identification and designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection (9403/08). There are however, uncertainties in this EU policy approach which remain unresolved. The literature and in particular Fritzon, Ljungkvist, Boinand and Rhinard (2007) argue that to fully ensure protection of critical infrastructures is virtually impossible as today's vital systems are too complex, and too vulnerable to a wide array of threats, to build absolute robustness with any confidence. It is however vital when looking at organizational civil emergency strategies that consideration is given to the possible impacts of interstate connections that may impact on the organization and make appropriate arrangements to deal with them.

2.3.4 Developing and Implementing a BCM Response

This section of the BCM lifecycle concentrates on the development and implementation of appropriate plans and arrangements to ensure organizational business continuity and the effective management of an incident.

2.3.4.1 Incident Response Structure

Organizations should according to The Standard, setup an incident response structure that enables an effective response and recovery from disruptions. This structure should be simple and quickly formed so that it will enable the organization to confirm the nature and extent of the incident, take control and contain the incident and communicate with the key stakeholders. This structure, often referred to as the Incident Management Team (IMT) or Crisis Management Team (CMT), should also be the trigger for any business continuity response. The IMT or CMT teams should have plans and procedures to help manage the incident and these should be supported by business continuity tools to enable continuity or recovery of critical activities. Plans should also be in place for the activation, operation, coordination and communication of the incident response.

The importance of teams in this context is noted by Janis (1982), as cited by Elliott, Swartz and Herbane (2010), who says that teams are important in the context of emergencies as they generally outperform individuals. Various names are proposed for the initial response team in the literature, Barnes (2001) calls the main incident response team the Emergency Management Team (EMT). He advocates letting the organizations structure chart guide the design of the team structure. The EMT is responsible for ensuring staff safety during any emergency, for declaring a disaster, for activating recovery teams and for managing the recovery effort. Barnes (2001) recommends that the EMT is made up of the most senior management with the CEO as overall EMT manager.

Elliott, Swartz and Herbane (2010) offer an alternate command and control structure for managing major events. They suggest that in order to ensure an organization's response to an incident is well managed a three tier structure, as used by the British police service, which contains three levels, bronze (operational), silver (tactical) and gold (strategic) is used. This structure will also facilitate dealing with the emergency services as they will already be acquainted with it. Whilst recommending the latter command and control structure, Elliott, Swartz and Herbane (2010) recognize that each organization may require their own specific structures. The figure below shows the three main phases (incident response, BC and recovery/resumption) over time of an incident, and the relationship between incident management and business continuity.

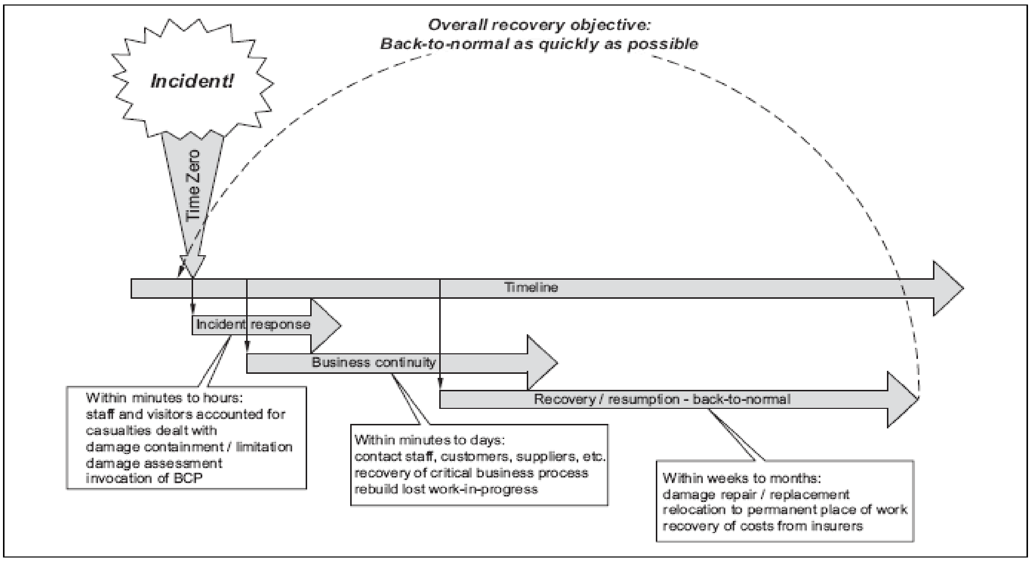

Overall recovery objective:
Back-to-normal as quickly as possible
Incident!
Time Zero
Timeline
Incident response
Business continuity
Recovery / resumption - back-to-normal
Within minutes to hours:
staff and visitors accounted for
casualties dealt with
damage containment / limitation
damage assessment
invocation of BCP
Within minutes to days:
contact staff, customers, suppliers, etc.
recovery of critical business process
rebuild lost work-in-progress
Within weeks to months:
damage repair / replacement
relocation to permanent place of work
recovery of costs from insurers

Figure 2.12: Incident timeline

(BSI 2006, Figure 2, p. 27)

The literature points out that there are several distinguishing characteristics that should be considered when making the decision to activate a BCM process, Dynes and Quarantelli (1977) note that the rate of decision making increases, as does the number of decisions made, particularly at lower levels of the organization. They identify that there seems to be less consultation among organizational members, and such individual autonomy means that organizational personnel and resources are committed quickly, often outside the organizations previous domain of competence. In their opinion, organizations usually lose autonomy when coming under the control of new "coordination" arrangements e.g. the Fire services; within organizations, sections with high crisis relevance gain decision making autonomy. Dynes and Quarantelli (1977) further note that organizational communication has to be seen as part of the decision making process and involves differentiation in content, channel and context. In general, under conditions of stress, social rather than technological factors are primarily responsible for impaired communication. The increase in technological forms of transmission during crises only increases the volume, and not the accuracy, of information, and hence, increases the need for collation and integration. The latter point is an important one for BCM. Filtering out unimportant communications in a crisis event is vital for those involved in recovery operations in order to ensure that the correct services are restored in the correct order and in the correct timescales. Superfluous communications will only hamper the recovery process.

All elements of organization should be involved in the incident management process to some degree. This is again where BCM is often seen as a unifying process which encompasses other disciplines such as Risk Management and Crisis management etc.

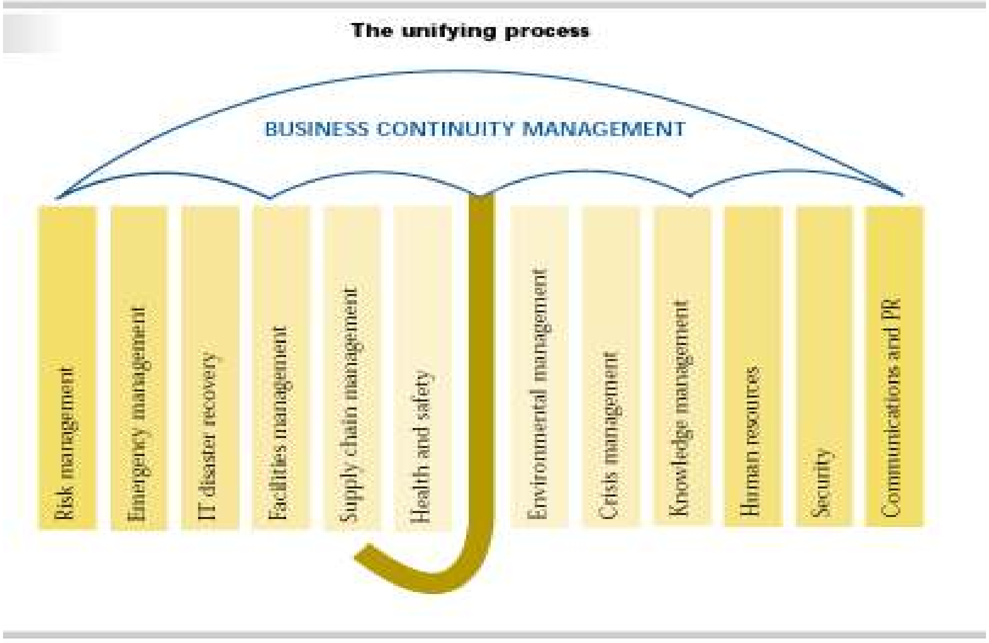


Figure 2.13: BCM: The Unifying Process,
(PAS 56 2003, p. 3)

The more an organization practices it BCM recovery process the easier it will be to invoke when a crisis happen, as Beatty (2007) points out, preparation is the key when responding to incidents. He also notes that an emergency is not just one single type of event but is often wide reaching and composed of many elements. The specifics of a recovery programme can often only be determined at the time a disaster occurs. They depend on the nature of the disaster, the point in time that the disaster occurs, and the anticipated period of disruption, Mayers (2006) and Fink (1986) refer to the fact that an effective crisis management plan pre-sets key decisions on the mechanical portions of the crisis – those aspects that rarely vary – and leaves an organization free to manage the content portion of the crisis relatively unfettered.

There is often no specific pre-set time between a crisis event happening and returning to full normal operation as each crisis event will present a different set of problems and issues for the effected organization. The Standard states that organizational recovery plans (plans that resume operations back to a normal state) may not be able to be implemented immediately as it may not be possible to define what "normal" is for a time after specific incidents. It recommends that organizations may therefore wish to have BC plans that allow extended operations so recovery plans can be put in place.

2.3.4.2 Content of Plans

The literature states that all plans, (incident management plans, business continuity plans, business recovery plans) need to be concise and accessible to those whose responsibilities are outlined in the plans. Each plan should contain details on its purpose and scope (as agreed by senior management), details of roles and responsibilities, information on how the plan is to be invoked, relevant contact details, task and action lists, resources requirements and copies of relevant forms and annexes according to BSI (2006). Any plans should also include prioritized objectives for the critical activities to be recovered, the recovery levels and timescales for the critical activities and a clear description of the situation in which each plan can be used.

It is important that the method by which any of these plans are invoked is clearly documented and understood so that they can be invoked as swiftly as possible.

Through practice and BCM exercises the organization should become more familiar and comfortable with the invocation of the various BCM plans.

2.3.4.3 The Incident Management Plan (IMP)

The IMP documentation allows the organization through its IMT, CMT, or EMT to manage the initial phase of an incident according to The Standard. The IMP according to BSI (2006) should contain details such as, task and action lists based on the BIA to ensure that further losses above the initial incident are prevented, information on how the organization will communicate with its stakeholders, lists of those responsible for first aid, employee communications etc. It is important that whatever its contents the IMP is modular and easy to use to ensure all the relevant information is to hand in the event of an incident.

In relation to predetermined incident management locations which are part of the IMP, Gallagher (2003) says that it should not be a question of seeking a venue when disaster strikes as a predetermined location is vital. Elliott, Swartz and Herbane (2010) suggest that for the CMT to be effective it must consist of people who will continually question decisions and information (devils advocates). It must have in place the relevant processes, people and communications channels to allow for quick and effective implementations. The inclusion of 'devils advocates' in the CMT is important as it ensures that all angles of a crisis are looked at and the relevant questions are asked at the appropriate time.

The move from emergency operations to recovery operations starts when the organization knows the location of the emergency and the initial estimates, or perceptions of the damage. As mentioned by Beatty (2007), emergency procedures must logically lead into recovery, business continuity procedures and activities.

2.3.4.4 The Business Continuity Plan (BCP)

The key purpose of a business continuity plan is:

> "to enable an organization to recover or maintain its activities in the event of a disruption to normal business operations… They may be invoked in

> whole or part and at any stage of the response to an incident.” (BSI 2006, p. 33)

Many formats of BC plan exist in the literature reviewed, but as Gallagher (2003) comments, while there are many formats, and software is available to provide assistance in setting up a BCP, there is no one format that fits all organizations. There are many and varied lists available outlining the recommended contents of a BCP and it is not intended to outline each of these in this literature review. However, it is worth noting that The Standard highlights some of the more crucial items that should be included in a BCP action plan. Checklists of prioritized actions and tasks highlighting, how the plan is invoked and by whom, how the decision to invoke is taken, who should be consulted/informed when making the decision to invoke the plan, how people are allocated, how the organization activates external or third party resources and where they are, how information is communicated and information on any manual workarounds or system recovery.

The plan should also identify the different resources (people, premises, technology, supplies, management of stakeholders and information) required at different points in time for the business recovery. Also included in the BCP should be the person(s) responsible for managing the BCP, up-to-date contact details for both internal and external contacts that might be required for support and incident logs to record information on decisions that are made during an incident.

What is appropriate for an organization depends on a number of factors, and in some cases the plan may be little more than a list of key contacts according to Gallagher (2003). Gallagher (2003) also warns against having a plan that is too complicated as this can be worse than having no plan at all and will most likely lead to the plans failure over time.

The features of a good plan as outlined succinctly by Gallagher (2003) are that it should be, simple, strategic, practical, probability (takes account of the probability of the plan being activated), flexible and easy to maintain. A balance therefore needs to be struck between having a hard to use overly detailed BC plan and having one that is to light on detail.

2.3.5 BCM Exercising, Maintaining and Reviewing BCM Arrangements

Throughout the literature the importance of exercising, maintaining and constantly reviewing BCM arrangements is emphasised. A robust BCM programme should ensure that an organization's BCM arrangements are validated by exercise, reviewed regularly and are kept up-to-date to ensure they are reliable. Gallagher (2003) notes that the rate of change and the ever increasing technological sophistication of the business environment provide significant challenges in the area of BCM. Keeping a plan updated and relevant is one of the most difficult tasks facing the business continuity coordinator. Some of the challenges faced by organizations as outlined by Gallagher (2003) are, regular reorganizations and reshaping; transformation, change and rationalisation processes; mergers and acquisitions; fast rates of technological change; increased dependence on just-in-time arrangements; greater levels of outsourcing; more flexible working practices; staff turnover and early retirement arrangements, which result in knowledge loss; hot-desking and virtual office arrangements.

All of the above impact on the ability of a BCM coordinator keeping the plan up-to-date and so it is essential that the BCM process is embedded in the organization in order to ensure it is kept current and subject to regular updates when organizational changes take place.

2.3.5.1 Exercise Programme:

As part of any BCM programme it is essential that an exercise programme is put in place that, over time will ensure that the BCP will work as anticipated. The importance of testing/exercising the BCP must be emphasised according to Gallagher (2003). An unexercised plan cannot be said to be viable or workable and will provide a false sense of security as issues will only become apparent if and when the plan is used in reality.

Exercising a BCP has multiple benefits for the organization according to The Standard. It will enable an organization to practise its ability to recover from an incident, verify that the BCP includes all critical activities, highlight any assumptions made that may need to be addressed, instilling confidence that the BCP works, raise awareness of BCM, validate the effectiveness and timeliness of restoration of critical activities; and demonstrate competence of the primary response teams and their alternatives. Bradbury (2008) advises that when testing is undertaken it is important to test the plans, the process, the people, and the infrastructure. The main test objectives are to exercise the recovery processes and procedures, familiarise staff with the processes and associated documents, verify that the documentation works, establish if the recovery objectives are achievable and identify improvements required to the strategy and processes.

Exercising plans can be undertaken in a number of different ways as suggested in the literature. Amongst the exercise options are: a desktop walk through, simulation exercises, component functional or rolling testing and a full live BCP test.

Some other test types that can be used according to Armit (2007) are: component test, ICT tests, cascade tests, callout tests, invocation tests, media tests, board level tests.

The exercise programme should ensure that all technical, logistical, administrative, procedural and operational system elements of the plan are exercised over time. It should also exercise the BCM arrangements and associated infrastructure and validate the ICT recovery plans including relocation of staff.

When approaching an exercise scenario, Gallagher (2003) recommends using a documented exercise plan which gives a clear idea of the objective of the exercise, those parties and resources that are involved, the expected exercise results and the times at which various exercise milestones should be achieved. The Standard notes that exercises need to be realistic, carefully planned and agreed with stakeholders to avoid risks of disruption during testing. All exercises should have clear aims and objectives and a debriefing meeting should take place after the exercise to learn lessons from it. BCP's and IMP's should be exercised to ensure completeness. The importance of learning from BCM exercises and testing is a crucial part of a BCM programme. Learning from incidents leads to better overall organizational resilience and it is important that when incidents occur, the BCM process captures this learning. As alluded to by Crichton, Ramsay and Kelly (2009), a key lesson extracted with hindsight from accident histories is that the affected organization(s) failed to learn from previous accidents and/or failed to recognize accident precursors that would have warned more insightful organizations of their drift towards disaster.

Testing and exercising of the BC plan ensures that the plan is continually ready in all aspects. Testing has four basis benefits according to Elliott, Swartz and Herbane (2010):

> " - Ensuring the organization can walk before it tries to run
> - Reducing complacency i.e. 'we have a plan so we are safe' attitude.
> - Improving maintenance and auditing
> - Maintains awareness."
>
> (Elliott, Swartz, and Herbane 2010, p. 249)

The need to conduct tests on a regular basis is evident from the literature. Alexander (2005) advises that plans should be tested and updated periodically on a repetitive cycle. Generally, a table-top or field exercise shall be conducted in order to test the plan at least once a year and a thorough revision shall be made at least once every six months. At this time details and data should be checked for accuracy and the plan "tuned" to ensure its optimum functionality according to Alexander (2005).

Each test undertaken further validates the content of the various BC plans and gives a level of assurance to the organization that the plans function as required should an event occur.

2.3.5.2 Maintaining BCM Arrangements

The literature states that, in order to keep BCM arrangements current a clearly defined and documented BCM maintenance programme needs to be in place to ensure that any changes, internal or external, that impact the organization are reviewed in relation to BCM. Any new products or services identified need to be assessed via BIA and RM to see if they are to be included in the BCM maintenance programme. The results of the BCM maintenance programme enable the organization to review and challenge any assumptions made in the BCM and will distribute updated or changed BCM policy, strategies, solutions, processes and plans under a formal change control process.

Maintenance according to Elliott, Swartz and Herbane (2010), is a generic term used to cover the activities necessary to see if the plan is up to date and relevant. They advocate that the BCP should be maintained regularly via testing or review. As outlined by The Standard, the BCM maintenance process should, document evidence of the management and governance of the organizations BCP, verify that key individuals required are trained, provide evidence that the risks faced by the organization are monitored and controlled and provide evidence that organizational changes have been included in the BCP and IMP.

2.3.5.3 Reviewing BCM Arrangements

As noted by Gallagher, (2003) and BSI (2006), while there is a large body of initial work to be undertaken, introducing risk-reduction measures, deciding on recovery strategies and creating the initial plans, the work will continue into the future but perhaps at a less intensely pace

The on-going commitment from senior management is essential as outlined by The Standard which advises that the continued top management input is required so that the BCM process is reviewed to ensure its continuing suitability, adequacy and effectiveness. The documented review should also ensure that the BCM policy complies with any relevant laws, standards, and regulatory requirements. It should address any required changes linked to policy or strategic shift or changes as a result of a BCM exercise. Reviews should take place periodically and can take the form of an internal or external audit or a self-assessment. These reviews will ensure that the BCM process is kept current and does not get forgotten by the stakeholders.

It is also essential that after initial BCM training has been completed an on-going programme of BCM training is put in place to keep the awareness of BCM alive within the organization. According to Gallagher (2003), as the business changes and plans change and staff come and go, the BCM training and awareness programme must continue and training is needed in the form of awareness programmes to ensure senior management commitment, practical training for those with roles in the plan, general staff training and specific training in the operation of the plans and in areas such as crisis, trauma management and counselling. Howe (2007) also recognises the need for continued BCM training stating that as the initial BCM project winds down the corporate culture should include on-going support from management in continuing to build on employee awareness and training, and active participating in recovery exercises, BCM programme updates and plan tests.

2.4 BCM and Organizational Resilience

As noted in The Standard, BCM provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.

When considering the research question ‘How has Business Continuity Management evolved in large Irish enterprises between 2004 and 2009’ it is essential that an analysis of the impact that BCM has had on Organizational Resilience (OR) is reviewed as there has been a distinct move in the literature to broaden the BCM perspective and to look to combine it with other disciplines such as risk, crisis and emergency management to create a more comprehensive approach leading to OR.

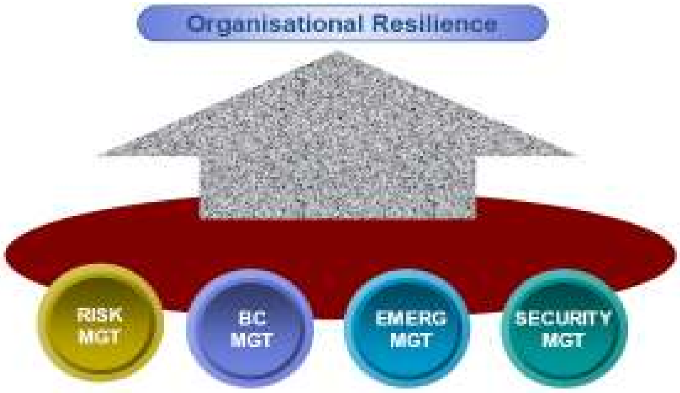


Figure 2.14: Organizational resilience as the integrated approach. (Oldfield 2008b, p. 6).

The word resilience is derived from the Latin words *resiliens* and *resilire* – first recorded in 1626 - meaning 'to rebound'. As stated by Oldfield (2008a), the word resilience may be preceded by: corporate, business, enterprise, emotional, individual, organizational, sectoral or societal. In each case the objective may be different: however each has common core elements, such as the ability to absorb change gracefully and remain stable in a turbulent environment.

2.4.1 Defining Organizational Resilience

Defining OR, Horne III (1997) states that it is the ability of a system to withstand the stresses of environmental "loading" based on the combination or composition of the system pieces, their structural inter-linkages, and the way environmental change is transmitted and spread throughout the entire system. Horne III (1997) further comments that to varying degrees, resilience is a fundamental quality found in individuals, groups, organizations, and systems as a whole. It allows a positive response to significant change that disrupts the expected pattern of events without resulting in regressive/non-productive behaviour. OR is therefore fundamentally about how flexible the organization is in coping with significant changes in the environment in which it operates.

2.4.2 The Characteristics of Resilience

Three fundamental characteristics seem to set resilient people and companies apart from others according to Coutu (2002). Having one or two of these qualities makes it possible to bounce back from hardship, but true resilience requires all three. The first characteristic as outlined by Coutu (2002) is the capacity to accept and face down reality. Doing this helps us train ourselves to endure and survive hardships. Second, resilient people and organizations possess an ability to find meaning in some aspects of life and values are just as important as meaning; value systems at resilient companies change very little over time and are used in times of trouble. The third characteristic of resilience is the ability to improvise. The ability to solve problems without the usual or obvious tools is recognised as a great strength.

Looking at OR from a BCM perspective it is sensible to look at those organizations that have resilience at their core, namely Highly Resilient Organizations (HRO's). Organizations involved in power provision, the oil industry and transport are most likely to be HRO's as the implications of failure in such industries carries huge consequences. Burke, Wilson and Salas (2005) define the main characteristics of a HRO as having, a sensitivity to operations, a reluctance to simplify, a pre-occupation with failure, a commitment to resilience and a deference to expertise.

2.4.3 Building Organizational Resilience

OR pervades many elements of an organization and sits across many organizational disciplines and processes including performance management, business excellence frameworks, organizational sustainability, BCM, DR and total quality management (TQM), according to Brouggy (2009).

Lengnick and Beck (2008) maintain that an organization's resilience capacity captures its ability to take situation-specific, robust, and transformative actions when confronted with unexpected and powerful events that have the potential to jeopardize an organization's long-term survival.

Referring specifically to BCM and OR, Jackson (2006) advocates using cross departmental teams to build OR and notes that approaching business continuity is part and parcel of general corporate planning, and by using a cross departmental team to own the concept, businesses can design and roll out their technology and processes with an element of continuity already built in. This approach will lead to higher levels of organizational resilience as resilience will be built into the process from the start. Having OR means that change (both good and bad) can be accommodated more efficiently within an organization. According to Lengnick and Beck (2008), alongside strategic agility, resilience capacity helps firms respond effectively to changing conditions, provides the basis for restoration after a severe jolt and can also offer an opportunity for an organization to undergo a positive transformation as a result of overcoming an exceptionally challenging experience.

Building a resilient organization presents many challenges as the safety and OR goals often conflict with other organizational influences. As stated by Skiver (2007), safety goals frequently become entangled with other organizational goals and safety is gradually downgraded over time in a continual battle for supremacy. Skiver (2007) further notes that when it comes to OR a significant role is played by the organizations business culture in that it provides the goals and boundaries to work within but is affected by external influences such as industry regulators, political decisions and particularly when it comes to safety, media interests and attention stirring popular opinion.

Some of the challenges of building OR into an organization as outlined by Skiver (2007) include: power struggles, incompatible goals, competence, censorship, business culture, management fads, academic discussions, failure to learn and short versus long term goals.

It is evident from the above list of challenges that building OR will therefore require an overall organizational commitment from top to bottom. As proposed by Arif (2007), resilience must permeate the entire organization. Dye and Langsett (2008) recognise the need for BCM to integrate and collaborate with other corporate functions involved in risk-related functions, such as IT security, physical security, privacy, enterprise risk management, contract compliance, supplier management, ethics and corporate governance.

An important requirement for most organizations today is having a resilient supply chain. Referring to organizational supply chains and resilience, Sheffi (2007) mentions that OR is dependent on having collaborative relationships with trading partners since the supply chain is only as strong as its weakest link.

In summarising what is required in order to build OR in an organization, the output from the National Organisational Resilience Framework workshop (2007) states that, resilience capability is strongest in an organization that anticipates and understands emerging threats, understands the threat impact, develops and maintains partnerships with critical stakeholders in their supply chain, sector and community, responds and recovers from disruptions as a unified organization team, adapts to disruptions and reacts flexibly to incidents, ensures staff are willing and able to support the organization in times of adversity, articulates clear organizational objectives, establishes a strong sense of purpose in response to and recovery from a disruption, leads with clear direction and enables devolved problem solving.

2.4.4 Determining the Organizations Resilience Capability

There are two important variables at play according to Sheffi and Rice (2005) when determining an organization's resilience, the competitiveness of the organization and the responsiveness of its supply chain. In competitive situations with low costs of switching an organization must be able to respond quickly or it will lose market share whereas an organization that is very responsive will be able to gain market share in a competitive environment or if it dominates it will be able to cement its dominant position. This is diagrammatically represented below:

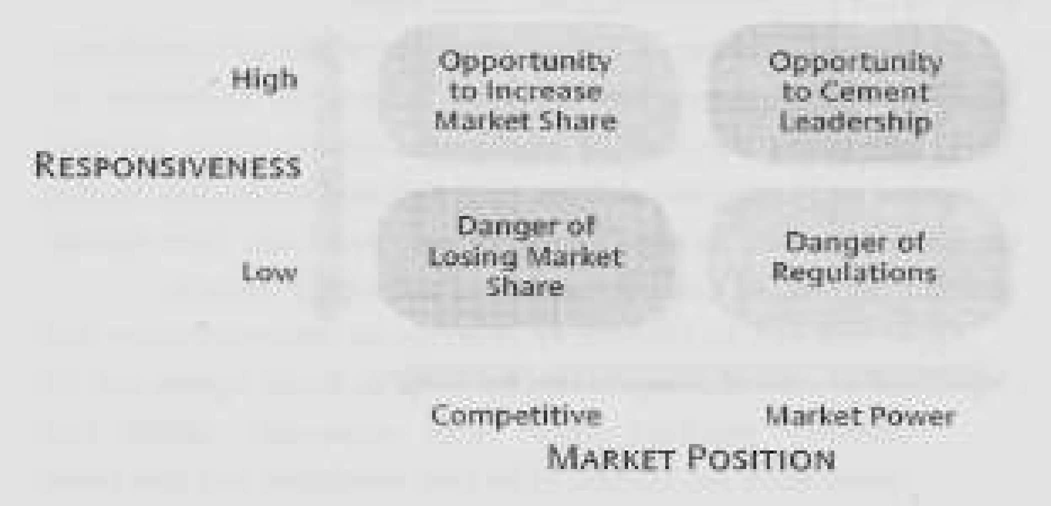

High
Opportunity to Increase Market Share
Opportunity to Cement Leadership
RESPONSIVENESS
Low
Danger of Losing Market Share
Danger of Regulations
Competitive
Market Power
MARKET POSITION

Figure 2.15: Company position and responsiveness
(Sheffi and Rice 2005, p. 45)

Today according to Sheffi (2007), due to tough competition and the range of choice open to customers, firms have to work harder and be more resilient than in the past as there are others waiting to take their place should they fail due to an incident.

When considering OR, Sheffi (2007) notes that it may not be productive to think too much about the underlying reason for disruption, instead the focus should be on what damage can be caused to the network (supply chain) and how this can rebound quickly. In this regard Sheffi (2007) recommends looking at resilient supply chains in industries that suffer disruption frequently such as high technology or fashion industries.

2.4.5 Becoming a Resilient Organization

When aiming for OR most organizations look to Highly Resilient Organisations (HRO's) such as nuclear power providers and air traffic control operators who have vast experience in the area as advocated by Burke, Wilson and Salas (2005). HROs have been described by LaPorte (1996) as being characterized especially by flexibility and redundancy in pursuit of safety and performance, where redundancy is defined by LaPorte and Consolini (1991) as the ability to provide for the execution of a task if the primary unit fails or falters. According to Roberts (1990), HROs use technical redundancy, where parts are duplicated (e.g., backup computers) and personnel redundancy, where personnel functions are duplicated (e.g., more than one person is assigned to perform a given safety check). Such HRO's build a strong safety culture, and can be more resilient to failure; they are pre-occupied with preventing failure, while more conventional organizations focus on their success. The latter interpret the absence of disaster as evidence of their competence and of the skilfulness of their managers. But, under the assumptions that success demonstrates competence, people can drift into complacency, inattention, and habitual routines, according to Crichton, Ramsay and Kelly (2009).

As with the BCM programme or any organization wide initiative programme, Burke, Wilson and Salas (2005) note that promoting OR is vital, particularly when working within a complex environment. Being proactive is not enough, organizations must also promote resilience in order to adapt to a wide range of situations. Burke, Wilson and Salas (2005) further state that there is an increasing need for organizations that operate in complex environments to be very efficient at 'expecting the unexpected', while at the same time remaining adaptive and able to contain the unexpected events that may still occur.

A framework of the antecedents, processes and outcomes associated with the transformation of a normal organization to HRO status is outlined by Burke, Wilson and Salas (2005). The theoretical framework that they present depicts the argument as to how organizations might make the transformation to HRO status via a team-based strategy. The primary theoretical foundation for this framework lies within (a) organizational change, (b) institutional theory and (c) HRO theory. The main focus of the theoretical framework is on the actual change process itself. In making the transition to becoming a HRO, existing organizational assumptions need to be changed in order to promote the values, beliefs and behaviours essential to catching the unexpected. Participation from employees throughout each stage of the process will better guarantee success.

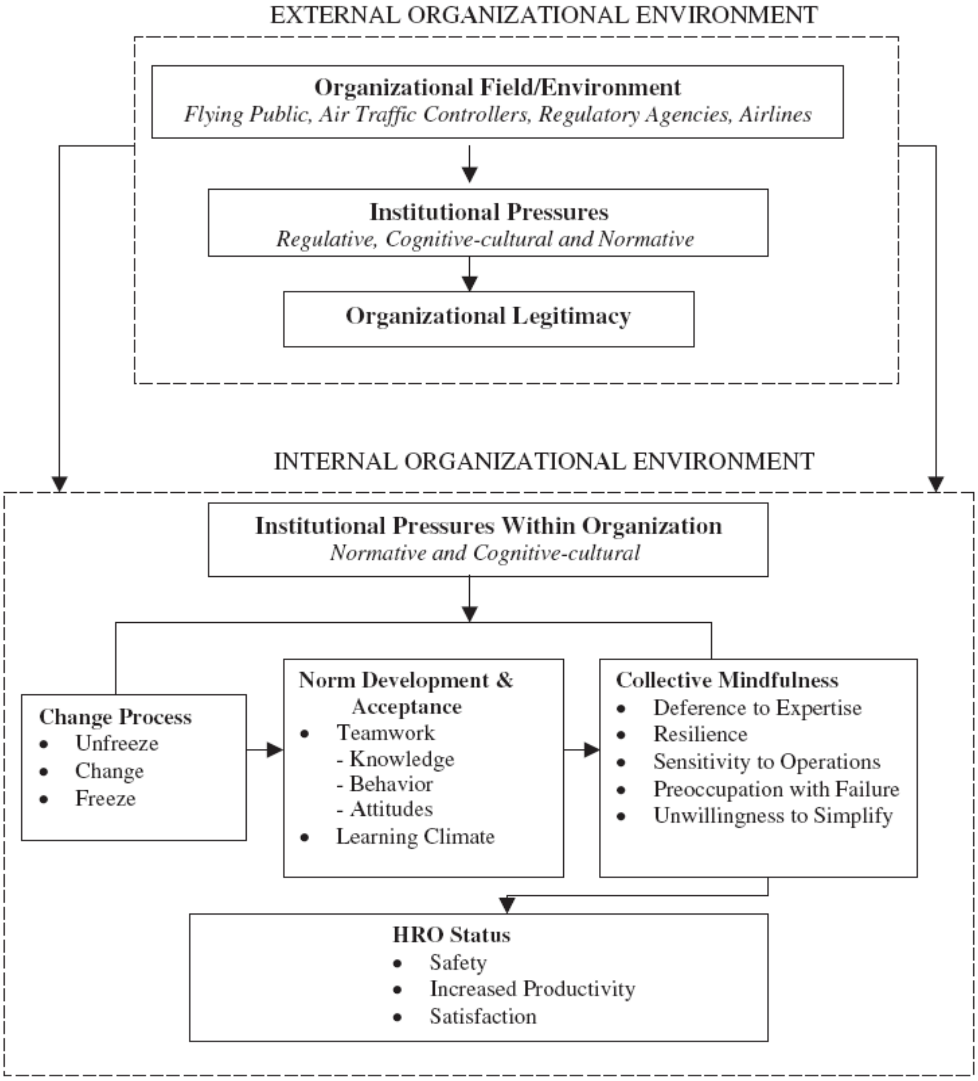

EXTERNAL ORGANIZATIONAL ENVIRONMENT
Organizational Field/Environment
Flying Public, Air Traffic Controllers, Regulatory Agencies, Airlines
Institutional Pressures
Regulative, Cognitive-cultural and Normative
Organizational Legitimacy
INTERNAL ORGANIZATIONAL ENVIRONMENT
Institutional Pressures Within Organization
Normative and Cognitive-cultural
Change Process
Unfreeze
Change
Freeze
Norm Development & Acceptance
Teamwork
- Knowledge
- Behavior
- Attitudes
Learning Climate
Collective Mindfulness
Deference to Expertise
Resilience
Sensitivity to Operations
Preoccupation with Failure
Unwillingness to Simplify
HRO Status
Safety
Increased Productivity
Satisfaction

Figure 2.16: Transformation to HRO.
(Burke, Wilson and Salas 2005, Figure 1, p. 511)

The steps in transforming an organization to a HRO as described by Burke, Wilson and Salas, (2005) are similar to those that take place during any change processes namely, "'unfreezing' the old way of doing business to jolt the organization into action, the actual change process then takes place through which the existing regulative, normative and cognitive-cultural systems are modified and then the final stage of the process is the 'refreezing' process where the new organizational forms, corresponding norms, values and behaviours gain traction.

Moving to a HRO footing will enable an organization to improve its BCM knowledge transfer capabilities. As Elliott (2009) argues, issues with knowledge transfer have had material effects in limiting the likelihood of translating new understandings (in the case of learning from disasters and crisis) into changed norms and behaviours within organizations. This is something that HROs try to combat through organizational learning.

As with a BCM programme, when creating a HRO the input from leadership is viewed as vital. Birk (2009) says that CEO involvement takes two primary forms, high-visibility leadership in promoting organizations' safety attitudes, behaviour and performance; and participation in industry-driven initiatives and activities whose results could be felt industry wide. La Porte and Consolini (1991) note that in HRO's, the leaders prioritize both performance and safety as organizational goals, and consensus about these goals is unequivocal.

In summary, when looking at OR Skiver (2007) says that the difference between a resilient and less resilient organization is how safety is managed in total where a resilient organization will focus on proactive safety management. Less resilient organizations will practice reactive safety management where savings from preventing accidents are rarely balanced with the costs of accidents. Essentially building a resilient organization is a question of systematic application of safety management principles, which in reality are always mediated by cost, prioritization and culture.

2.5 Conclusions

The main conclusions drawn from the literature review are that the understanding of what constitutes organizational resilience, the challenges of achieving it and its benefits in a BCM context are well documented in the literature particularly in relation to HROs. Having good programme management processes in place is a clearly identified as a vital component for a successful and an effective BCM programme. The importance of the participation and backing of senior management is crucial for the success for any BCM programme. This backing must be maintained and emphasised throughout the lifetime of the BCM programme and not just at the start. A BCM programme is highly influenced by the strategy adopted by the organizations senior management according to the literature and the BCM professional needs to be aware of the strategy of the organization when implementing and maintaining the BCM programme. Culture both in terms of the business and the internal culture of the organization have an important part to play in the way BCM is approached and also impact the programme during its lifetime. Changes in the business and organizational culture have an inevitable impact on the BCM programme which needs to be part of the overall organizational change management process in order for these changes to be successfully accommodated. The causes, challenges of crisis events and understanding of their impacts from an organizational perspective via the BIA are well documented in the literature and need to be taken into considered when implementing a BCM programme. The ever increasing and expanding usage of technology in organizations and the interconnection of organizations and countries as highlighted in the literature are creating greater BCM issues that merit consideration by the BCM profession. Consideration therefore needs to be given to the impacts of crisis events on the wider organizational supply chains and the need for robust supply chains is evident in the literature. The overlap between Risk Management, Crisis Management and BCM and the central importance of these to an organization is evident in the literature. Their priority depends however on the point of view of the writer of the article.

It is noteworthy that there are a lack of articles specifically addressing the BS25999 standard and it shows the low level impact of The Standard on the academic/research community to date. A study by Elliott and Johnson (2010) notes that BS25999 and audit proved to be of great interest and concern to respondents but also that few respondents viewed BCM as a strategic activity.

This chapter reviewed the literature on BCM using the stages of the Business Continuity Lifecycle as a structure around which the review was based. The literature review identified and discussed what has been proposed as constituting good practice in terms of BCM and an analysis of the impact that OR has had on BCM. The chapter ended with conclusions drawn from the literature. The next chapter will outline the research methodology used for this research.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter places the research within its relevant philosophical and methodological context and takes into consideration the different perspectives that provide the foundations in the search for knowledge and understanding and positions this research within this context. The chapter will also detail the approach used when gathering the material and data required to answer the research question and a rationale for the methods selected.

3.1.1 Research Overview

Choosing the appropriate method to gather the information helps to ensure that the data is valid and robust. Any theory or research question will only be tested if the research is designed and grounded in the correct research strategy and with the use of the correct methodology.

Remenyi (1998) highlights several benefits of a well thought out research strategy. He describes how it enables communication and replication between researchers which in turn protects against unintentional mistakes. It ensures a logical structure which will have appropriate empirical and reasoning components.

This chapter explains the reason why a particular research philosophy was selected and details the research design and strategy. The research onion as developed by Saunders (2007) was selected as an appropriate model for this research.

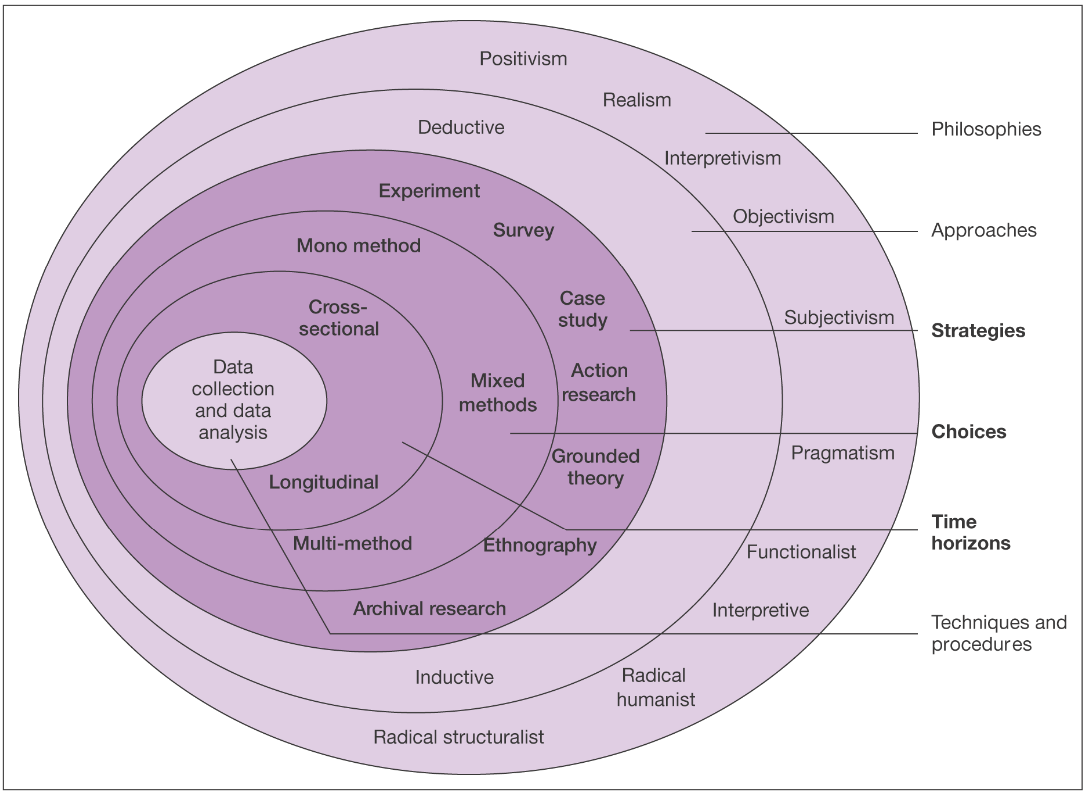


Fig 3.1: The research 'onion'

(Saunders, Lewis and Thornhill, 2007, p 102)

In summary the design of the research strategy is important if the findings are to have genuine credibility and use.

3.1.2 Research Philosophy.

Research philosophy:

> "relates to the development of knowledge and the nature of that knowledge" (Saunders, Lewis and Thornhill, 2007, p 101).

Galliers (1991) notes that the two major research philosophies that have been identified in science are, Positivism (sometimes referred to as scientific) and Interpretivism (also known as anti-positivist).

Positivism:

This stance assumes there exists an objective social reality that can be studied independently of the action of the human actors in this reality, according to Khazanchi and Munkvold (2000). Positivism is where data has to be observed, proof is the hallmark of this approach. This type of research is similar to a natural science approach where only observable facts will lead to the production of data. Positivism culminates in law-like generalisations. Research is undertaken as afar as possible in a value-free way according to Saunders, Lewis and Thornhill (2007) in order to ensure that bias from the stakeholders in the research will be minimised.

Interpretivism:

According to Khazanchi and Munkvold (2000) this stance assumes that reality and our knowledge thereof are social constructions, incapable of being studied independent of the social actors that construct and make sense of reality. Interpretivism has a focus on people rather than definite tangible objects. In this approach the reviewer should adopt an empathetic stance and should try to understand the world from the perspective of the population being studied.

In summary it has been observed by Benbasat et al, (1987) that no single research methodology is intrinsically better than any other methodology, some authors, such as Kaplan and Duchon, (1988), call for a combination of research methods in order to improve the quality of research. As noted by Saunders, Lewis and Thornhill (2007) business and management research is often a mixture between positivism and interpretivism. By its nature this study tries to avoid what may be characterised as methodological monism, i.e. the insistence of using a single research method. This is not due to any indecision between the differences of the various alternatives, instead it is based on the belief that all methods are valuable if used appropriately and that research can include elements of both the positivist and interpretivist, approaches, if managed carefully.

3.1.3 Research Approach.

Research approaches normally consists of two options, Deductive and Inductive, and it is important to consider whether a particular research project should use the deductive approach which deduces reality from the data, where the researcher is independent from the study and owes much to the scientific approach or whether your research uses the inductive approach where reality is induced from the data and the researcher is part of the research process.

Deductive:

The deductive approach deduces reality from the data. Saunders, Lewis and Thornhill (2007) note that it involves the development of a theory that is subject to a rigorous test. Quantitative data is used and the approach is a highly structured one where the researcher is independent from the study. The deductive approach uses scientific principles and searches to explain causal relationships between variables.

Inductive:

The inductive approach is where reality is induced from the data and the researcher is part of the research process. It draws context and understanding from the events observed in the research. Qualitative data is used as is a flexible structure for data collection and analysis.

When viewed against the research philosophies, deduction owes more to positivism and induction to interpretivism.

Looking at the research question posed: How has BCM evolved in large Irish enterprises between 2004 and 2009? It is considered vital that deductive data is used and that this is backed up by further inductive data to produce a more rounded, in depth explanation of the results.

3.1.4 Research Strategy.

A number of research strategies have been identified by various writers. Saunders, Lewis and Thornhill (2007) identifies them as being experiment, survey, case study, action research, grounded theory, ethnography and archival research.

Experiment: Used when an experiment population and a control population are mixed and randomly assigned a variable. The measured change will be solely due to the variable. This is not viewed as suitable for management research and therefore not applicable to this research.

Survey: Allows for a collection of large volumes of information when specific questions are posed for exploratory research. Surveys enable the researcher to obtain data about practices, situations or views at one point in time through questionnaires or interviews. Quantitative analytical techniques are then used to draw inferences from this data regarding existing relationships. The use of surveys permit a researcher to study more variables at one time than is typically possible in laboratory or field experiments, whilst data can be collected about real world environments. The survey can also be broad enough to allow a variety of questions to be posed where opinions are required as well as tangible data. As noted by O'Leary (2004) a good survey has the potential to reach a large number of respondents; generates standardized, quantifiable, empirical data - as well as some qualitative data; and offers confidentiality and anonymity

A key weakness when using a survey is that it is very difficult to realise insights relating to the causes of or processes involved in the phenomena measured. There

are, in addition, several sources of bias such as the possibly self-selecting nature of respondents, the point in time when the survey is conducted and in the researcher him/herself through the design of the survey itself.
The survey method favours deductive research and is deemed a suitable strategy for this research in order to find out what is the current practice in BCM amongst the respondents.

Case study: Permits evidence to be gathered with a selected entity when the actual context is not very clear from the outside. The study can be further divided in examining an organisation as a whole, examining more than one organisation or what is referred to as an embedded case study, examining units or departments within the organisation. An important feature of a case study is the requirement for ensuring the data collected can be verified by other data gathering within the context of the case study. As the area is still developing the research from a case study may not be as insightful as a survey. Case studies can be considered weak as they are typically restricted to a single organisation and it is difficult to generalise findings since it is hard to find similar cases with similar data that can be analysed in a statistically meaningful way. Furthermore, different researchers may have different interpretations of the same data, thus adding research bias into the equation. The case study was not considered an appropriate strategy for this research.

Action research: Concerns research conducted during change within that organisation. It occurs in a dynamic environment where the change being studied is taking place and the organisation and all the stakeholders within it are part of that change. Through direct intervention in problems, the researcher aims to create practical outcomes while also aiming to re-inform existing theory in the domain studied. As with case studies, action research is usually restricted to a single organisation making it difficult to generalise findings, while different researchers may interpret events differently. The personal ethics of the researcher are critical, since the opportunity for direct researcher intervention is always present. It would be a good system for observing the process of introducing a BCM model into an organisation however it is not an appropriate form of research for this study.

Grounded theory: Utilises an inductive approach and builds a theory as the research is being conducted. The theory is grounded to the data as it is being gathered. This is not appropriate to the research question posed in this research as the hypothesis is already defined and there is no proposal to define a theory.

Ethnography: Is a research strategy that adopts an inductive approach over a long period. The researcher is immersed in the research question and high levels of observation are required. The characteristics of the research question will require answers rather than observations. This form of research is not appropriate to this study.

Archival research: Uses the review of records and documents as a primary information source. This area of research is novel and there is unlikely to be enough of archival information in place to support a dissertation so it has been discounted as a research strategy for this research.

As outlined by Bell (2005) for each method considered asking – Is this the best way of obtaining the information? Each of the research strategies above will involve one or more data collection methods.

3.1.5 Research Time Horizon.

For this research the time horizon consisted of two snapshots of the evolution of BCM in large Irish enterprises taken in 2004 and 2009.

3.1.6 Data Collection Methods.

According to Bell (2005) the first question in choosing the appropriate data collection methods is not 'Which method" but rather "What do I need to know".

To answer the research question How has BCM evolved in large Irish enterprises between 2004 and 2009? fully it is vital that the following questions are answered.

1: What data is needed to answer the research question?

2: Who has the information required to answer the research question?

3: What research instruments will be used to retrieve the relevant data?

4: How will the data retrieved be analysed?

3.1.6.1 What Data is needed to answer the Research Question?

In order to provide a comprehensive answer to the research question it was important to ascertain the attitudes and approaches taken to BCM in the respondent organizations.

This included gathering information from the organizations on:

- The drivers of BCM;
- To whom is their BCM capability communicated;
- The types of disruptive events that were experienced;
- The extend of disruption caused by certain events;
- Whether BCM plans exist;
- The extent of their BCM plans;
- Where does the responsibility for BCM lie;
- How is outsourcing handled in their BC plans;
- The sources used for gathering BCM information;
- Whether the BS25999 standard is used in forming BCM plans;
- The frequency and depth of BCM exercises undertaken;
- The status of BCM budgets.

One of the key areas in maintaining mission critical activities is power management. Included here was the gathering of information on:

- Experience of power outages;

- Whether power issues are covered in BC plans;
- The extent of generator and UPS use;
- The extent of generator and UPS use amongst the respondents outsource suppliers.

Information Technology Service Management (ITSM) has gained importance within organizations since the 2004 survey and as it contains a BCM element it was deemed necessary that information was retrieved on this process and how it was implemented in the respondent organizations.

In order to assist in the classification of the respondent organizations the following information was gathered:

- The industrial sector in which the organization operates;
- The area in which the organization operates;
- The annual turnover and number of employees;
- The size and status of the organization.

3.1.6.2 Who has the information required to answer the research question?

The research population was taken from a list of organizations using a sales and marketing contacts database of large Irish organizations used by Renaissance Ltd a leading Irish IT security distributor and business continuity consultancy provider combined with the Irish Times top 1000 companies in Ireland list. In 2004 one hundred and twenty questionnaires were issued to the largest companies and a total of fifty two questionnaires were returned and these formed the basis of the analysis and findings. This represented a 43.33% return.

By 2009, of the fifty two original organizations who responded in 2004, eight no longer operated in Ireland, had ceased to trade, were closing or had undergone mergers, thus forty four organizations were surveyed again for the second study. Of the forty four surveys sent twenty eight (63%) responses were received and deemed relevant for this research. Where possible the survey questionnaire was sent to the original respondents within each organization.

3.1.6.3 What Research Instruments Were Used to Retrieve the Data?

There are three forms of information that are generally accepted as valid sources for research.

- Primary – original or first occurrence of material that has not been previously analysed. This can, for example, take the form of data gathered during interviews or via questionnaires.
- Secondary – this type of information is created from primary material and contains an interpretation of original material. Information in this form is usually contained in textbooks, journals and reviewed articles.
- Tertiary – these act as tools in understanding and locating information. Here the information is contained in databases, dictionaries, bibliographies etc.

Secondary and tertiary resources, in the form of published articles, documents and literature, were used to take the first steps towards answering the research question, to place the research in its academic context and to provide a benchmark against which the research results could be compared. According to Bell (2005) most research projects will require some analysis of documents. This may be used to supplement other methods or may be the central or only method. It is a useful method when the researcher does not have access to the subjects of the research. This secondary research consisted of reviewing the pertinent literature available on the subject. The literature included an in-depth study of journals, articles and research literature. Each document analysed was subjected to a critical examination. The academic literature was, where relevant, supplemented by the research and good practice guidance published by relevant professional bodies.

In order to collect primary data the researcher used a survey questionnaire and a series of interviews. According to Denscombe (2007) questionnaires are most productive when there are large numbers of respondents in many locations, when the information required tends to be straightforward, brief and uncontroversial, where open and honest answers are possible, where there is a need for standardised data from identical questions and where respondents can be expected to be able to read and understand the questions.

Survey Questionnaire

Denscombe (2007) notes that survey questionnaires have both strengths and weaknesses. They can be used as a cost effective means of data collection are easy to analyse due to their common format, are familiar to most people, reduce bias to uninformed question presentation and are less intrusive than face to face or telephone surveys. On the downside they may be subject to low response rates, do not allow an ability to probe responses (unless comments are allowed which partially overcomes this), are incapable of capturing gestures and visual clues, may not be completed by the person to whom they were sent and are not suitable for some e.g. where literacy skills are poor. Despite these issues a survey questionnaire that is properly designed will overcome these difficulties and enable the relevant data to be collected.

As outlined by Rugg and Petre (2007) when conducting a questionnaire the first issue is selecting the correct list of questions. The questions for the survey were derived from the preliminary list of data (as outlined in section 3.1.6.1) required to answer the research question and these data items were drawn from the Chartered Management Institute (CMI) survey, supported by the Civil Contingencies Secretariat and the Business Continuity Institute (BCI), which has been run on an annual basis in the UK for the past 10 years as was the questionnaire approach and structure.

The survey questionnaire was designed and laid out in a clear concise manner and using simple and unambiguous language in order to ensure that the required data was collected as accurately as possible and to avoid the answers being contaminated, distorted or uniformed as outlined by Saunders, Lewis and

Thornhill (2007). The question types consisted of list questions where one or more responses could be selected, category questions where each respondents answer could fit only one category and two rating questions used to collect opinion data. In 2004 the majority of questions the layout and sequence were taken from the CMI annual survey as research indicated that no similar survey had taken place in Ireland so the survey was run to see what results would be found in an Irish context. Saunders, Lewis and Thornhill (2007) mention that when designing individual questions adopting questions used in other questionnaires is an efficient method rather than developing your own questions and can allow for comparisons between separate studies. The survey questionnaire was eight A4 pages in length, as found by Saunders, Lewis and Thornhill (2007) in general a length of between four and eight pages is acceptable for a self-administered questionnaire

Interviews

According to Bell (2005),

> 'Moser & Aron (1972) describe the survey interview as 'a conversation between interviewer and respondent with the purpose of eliciting certain information from the respondent'…the attainment of a successful interview is much more complex than this statement might suggest.'
> (Bell 2005 p157).

Bell (2005) also notes that interviews have both strengths and weaknesses. Their strengths lie in the fact that interviews can yield rich material, a skilful interviewer can follow up ideas during the interview, non-verbal communication can also provide information and responses can be developed and clarified. The data quality issues inherent in interviews include reliability, forms of bias and validity and generalizability according to Saunders, Lewis and Thornhill (2007).

The interviewer ensured that these data quality issues were borne in mind when undertaking the interviews by ensuring that set questions were asked in a predetermined order and that none of the interviews were allowed to deviate from the set list of questions in order to avoid the answers being contaminated, distorted as outlined by Saunders, Lewis and Thornhill (2007).

Mixed Methods

According to Curran and Blackburn (2001) as cited in Saunders, Lewis and Thornhill (2007) the choice of multiple methods for data collection is increasing advocated within business and management research, where a single research study may use quantitative and qualitative techniques and procedures in combination as well as use of primary and secondary sources. As Tashakkori and Teddlie (2003) as cited in Saunders, Lewis and Thornhill (2007) argue, multiple/mixed methods are useful if they provide better opportunities for the researcher to answer the research questions and where they allow a better evaluation on the extent to which the research findings can be trusted and inferences made from them.

There are two major advantages for using multiple/mixed methods according to Saunders, Lewis and Thornhill (2007). Firstly different methods can be used for different purposes in a study. In the case of this research the mixed method research used a sequential approach using firstly the survey followed by the interviews based on the key themes derived from the survey. Secondly different methods enabled triangulation to take place. In the case of this research the interviews acted as a crosscheck of the survey findings. This approach had the following benefits:

> "The extent of your data collecting will be influenced by the amount of time you have…Even so, if possible, efforts should be made to cross-check findings, and in a more extensive study, to use more than one method of data collecting. This multi method approach is known as triangulation." (Bell 2005 p. 116)

The approaches to data collection applied in this research could have been used together or on their own but for this research they were combined, to provide triangulation, in order to enhance the reliability and validatity of the research findings.

3.1.7 Data Analysis and Data Reliability

3.1.7.1 Data Analysis

The terms quantitative and qualitative are used widely in business and management research to differentiate both data collection techniques and data analysis as mentioned by Saunders, Lewis and Thornhill (2007). This research uses both forms of data collection techniques in the form of a survey and also interviews. Saunders, Lewis and Thornhill (2007) say that one way to distinguish between the two techniques is the focus on numeric or non-numeric data. Quantitative is predominately used as a synonym for any data collection technique (such as a questionnaire) that generates or uses numerical data. In contrast qualitative is used for any data collection technique (such as interview) that generates non-numeric data.

Quantitative data: As referred to by Saunders, Lewis and Thornhill (2007) quantitative data in its raw form conveys very little meaning to most people. According to O'Leary (2004), quantitative techniques use an investigative approach that results in numeric data and is valuable when highlighting percentages, obtaining measurements and testing hypotheses. The data needs to be processed to make it useful in order to turn it into information. Quantitative techniques such as graphs, charts and statistics are used to do this to enable the researcher to explore, present, describe and examine relationships and trends within the data. The quantitative data returned from this survey can be classed as nominal data according to Saunders, Lewis and Thornhill (2007) definition. Nominal data is data that involves simply counting the number of occurrences in each category of a variable. For virtually all analyses the categories should be unambiguous and discrete thus preventing questions as to which category an individual case belongs to.

The survey questionnaire included a total of 33 questions (see Appendix A for survey outline) and was broken down into the following sections:

- Exploring Business Continuity Management;

- Power Management;
- Information Technology Service Management (ITSM);
- Classification and Profile of Organizations including location, size, turnover.

After gathering the completed survey questionnaires from the respondents, total responses for each individual part of each question were extracted, and input into a data matrix using Microsoft Excel spread sheets for analysis and tabulation. The number of responses to each part of each survey question were counted using a simple binary coding method (1 for a positive result and 0 for a negative), averaged and displayed as a percentage of the overall number of replies to each specific question. Any missing data was recorded with a 0 coding, signifying a null response. As noted by deVaus (2002) there are four main reasons for missing data: the data was not required from the respondent, perhaps because of a skip generated by a filter question in the survey, the respondent refused to answer the question, the respondent did not know or have an opinion on the question being asked or the respondent may have missed the question by mistake. This process mirrored the approach taken in the 2004 survey to ensure that the results from both surveys were comparable. The results obtained were then charted and labelled clearly using Microsoft Excel for presentation and were compared and analysed against the 2004 survey results to show the trends over time and therefore the evolution of BCM in large Irish Enterprises between 2004 and 2009. These results are presented in Chapter 4.

Qualitative Data: Saunders, Lewis and Thornhill (2007) note that qualitative data refers to all non-numeric data or data that has not been qualified and can be a product of all research strategies. This form of data can range from a short list of responses to open-ended questions or more complex data such as interview transcripts. According to Saunders, Lewis and Thornhill (2007) the data is normally based on meanings expressed through words, with results in non-standardised data requiring classification into categories and having analysis conducted through the use of conceptualization. O'Leary (2004) says that this investigative approach results in descriptive textual information. The interview data created by this research is a case in point.

Interviews were completed following the survey questionnaire. The purpose of these interviews was to explore in more depth the main findings and themes that emerged from the survey. As noted by Carson, Gilmore, Perry and Gronhaug (2001) the interview provides a purposeful discussion between two people. This was important as it built on the understanding of the survey data and provided a broader qualitative view.

For the qualitative data in this research a manual data analysis process took place for each of the recorded responses to the specific interview questions. At the start of each interview the name of the interviewee was recorded in order to provide an accurate record of the interview. As each question was asked the number of the question was read out by the interviewer in order to provide further clarity for analysis. Each audio file was also time and date stamped for accuracy. The interview questions used were based on the key themes derived from the quantitative survey and those which emerged during the literature review. The interviews were used to provide an insight from different perspectives within the BCM industry in Ireland.

The recorded responses to the interview questions were subsequently transcribed and then coded according to the key themes from the survey and the literature.
The coding included:

- The drivers for BCM within the organizations;
- To whom is their BCM capability communicated;
- The types of disruptive events that were experienced;
- The extend of disruption caused by certain events;
- Whether BCM plans exist;
- The extent of their BCM plans;
- Where does the responsibility for BCM lie;
- How outsourcing is handled in their BC plans;
- The sources used for gathering BCM information;
- Whether the BS25999 standard is used in forming BCM plans;

- The frequency and depth of BCM exercises undertaken;
- The status of BCM budgets.

The coded material was then grouped together so that a general answer to each question could be gleaned.

3.1.7.2 Data Reliability

Reliability as outlined by Saunders, Lewis and Thornhill (2007) refers to the extent to which the data collection techniques or analysis procedures will yield consistent findings. Bell (2005) notes that in order to ensure reliability the researcher should ask themselves whether another researcher using the same research instrument and asking the same questions would get the same or similar responses.

The survey questionnaire and the interviews used in this research were designed such that respondents would be required to answer the same set of questions in a pre-determined order as mentioned by Carson, Gilmore, Perry and Gronhaug (2001). The design of the survey questionnaire considered the approach and structure used in the annual Chartered Management Institute (CMI) survey, supported by the Civil Contingencies Secretariat and the Business Continuity Institute (BCI), in the UK.

In order to ensure the reliability of responses to the surveys each question was carefully designed to ensure only specific responses could be received, the layout of the questions and the questionnaire was clear and concise and based on the CMI survey layout. Each respondent received a clear explanation of the purpose of the questionnaires. A further test of reliability arises from the fact that where possible the original respondents were sent the survey questionnaire in both 2004 and 2009 ensured that as outlined by Mitchell (1996) a test re-test of reliability was obtained by comparing the data collected with those from the same questionnaire collected under as near equivalent conditions as possible. In other words the questionnaire was administered twice to the respondents where possible. See Appendix A for the Survey Cover letter and questionnaire outline.

It should be noted that before final circulation, the survey was piloted with BC and academic specialists who were not working in large organizations, and therefore fell outside the survey population. Each of the individuals offered suggestions that helped refine the survey and offered advice regarding clarity and relevance within the questions. The researcher revised the survey questionnaires based on the suggestion of the respondents. The researcher then excluded irrelevant questions and changed vague or difficult terminologies into simpler ones in order to ensure comprehension. This process endeavoured to ensure 'content validity' as outlined by Saunders, Lewis and Thornhill (2007) which is the extent to which the questions in the questionnaire provide adequate coverage of the investigative questions.

The surveys were self-administered and sent via post. A cover letter also accompanied each survey. Each survey questionnaire was individually numbered to ensure a record could be kept of those who had responded, as advised by deVaus (2002). This meant that it was possible to ensure that the 2009 survey was sent to the respondents to the 2004 survey. These respondents consisted of Directors, Chief Information Officers, Information Technology Directors, Business Continuity Managers and Information Technology Managers which ensured that where possible no uninformed responses were received as highlighted by Saunders, Lewis and Thornhill (2007).

As noted by Maxwell (1996), interviews can prove highly subjective however, audio taping, transcription of interviews, and taking detailed notes during the interview process served to enhance their validity. The interviews undertaken as part of this research were held face to face with respondents and used both audio taping and note taking in order to ensure their validity. Interviewees were issued with the questions in advance of the actual interviews taking place. See Appendix B for the Interview questions.

According to Saunders, Lewis and Thornhill (2007) there are a number of data quality issues that can be identified in relation to the use of interviews related to, reliability, forms of bias and validity and generalizability. As alluded to by Marshall and Rossman (1999) as cited in Saunders, Lewis and Thornhill (2007), these issues of reliability are often outweighed by the fact that it is not necessarily intended that these interviews are repeatable since they reflect the reality at the time they were undertaken in a situation that may change. The audio tapes and the notes taken during the interviews were retained in order to ensure their validity and to enable other researchers to refer to them in order to understand the process that was used and the findings derived and where appropriate, to enable them to reanalyse the data collected. Saunders, Lewis and Thornhill (2007) note that forms of bias in an interview can occur in three ways, interviewer bias, interviewee bias and response bias. In order to control any occurrence of bias the interviewer ensured that only the questions as outlined were asked and that the interviews were conducted in as structured a way as possible using standardised questions asked in a predetermined order to ensure as consistent a response as possible. In relation to generalizability issues the fact that the interview questions were derived from the main themes of the survey and the literature review ensured that the interviews did not run in a generalized way but were instead focused on the relevant topics. All survey responses were retained alongside the spread sheets used for analysis as have the digital audio file recordings of the interviews.

3.1.8 Research Summary

The research therefore consisted of document analysis, a survey questionnaire, and interviews. This combination allowed for the successful collection of the data required for the original research project and the same research instruments were deemed appropriate for retrieval of the relevant data in order to answer the research question and to allow a comparison of the two surveys results to take place.

3.2 Research Ethics

There is growing acceptance of the power inherent in creating knowledge as noted by O'Leary (2004). With this acceptance comes acknowledgement of the need for ethical and political awareness to be a mainstream consideration in the research process.

The values of DCU as a university are expressed in their code of ethics for research. This code requires researchers using human participants to examine the relationship between the researcher, participant and topic to access the potential for any ethical issues to emerge.

As this study required the participation of human respondents, specifically BCM professionals, the consideration of ethical issues was necessary for the purpose of ensuring the privacy as well as the safety of the participants. The significant ethical issues that were considered in the research process include consent and confidentiality. In order to secure the consent of the selected participants, the researcher relayed all important details of the study, including its aim and purpose. By explaining these important details, the respondents were able to understand the importance of their role in the completion of the research. The respondents were also advised that they could choose not to participate in the study if they wished. The confidentiality of the participants was also ensured by not disclosing their names or personal information in the research. Only relevant details that helped in answering the research questions were included.

3.3 Chapter Summary

This chapter presents a detailed account of the research philosophy, strategy and methodology according to which the research was conducted. The research was placed in both the positivist and the interpretivist camps, utilising a mixture of survey and interview research approaches. Previous literature describing surveys is valuable in identifying the salient points of the survey methodology, as well as illustrating the weaknesses associated with it. An explanation was given as to how the proposed two mixed methods would interoperate so as to achieve the research objectives alongside a substantial literature review which was conducted in order to understand the BCM concept and to enable the author to get a better understanding of its current application.   These are explained in greater detail elsewhere in the thesis. The practical side of the thesis was detailed recounting how suitable respondents were identified for the research and detailing the broad procedures for data analysis and data reliability.

By following the methodologies outlined it would be possible to conduct a similar study using a different set of respondents as mentioned by Creswell (1994), thereby adding to the body of literature on this particular subject.

In conclusion the outputs from the literature review, the survey and the interviews were combined to enable the creation of conclusions and recommendations based on the research data retrieved. The next chapter will outline the results of the survey which has been undertaken for this research and will endeavour to show that the conclusions garnered from the literature review are backed up in reality.

CHAPTER FOUR

RESEARCH ANALYSIS AND RESULTS

4.1 Introduction

In this chapter the results of the research survey (from 2004 to 2009) returned by the participating organizations are presented, matched against the research objectives and discussed. Tables are used to present the results of the surveys. The results provide an insight into how the focus and experiences towards business continuity management (BCM) have evolved in large Irish based organizations over the five year period. The survey also assists in providing a more in depth insight into the organizations BCM strategies and examines the extent to which BCM has been implemented within the organizations. The results also expand the understanding of BCM and how it plays a part in the wider process of Organizational Resilience (OR). The specific areas of information technology service management (ITSM) and power supply are also included in the study to expand the understanding of BCM and resilience.

The presentation and discussion of the main research findings follows along with a comparison of the results against those of the original 2004 survey.

4.2 Results of the Survey Analysed

In order to provide an overview of the respondents and the organizations surveyed, the following section includes data relating to industrial classification.

4.2.1. Classification & Profile of Organizations

This section of the survey included six questions (questions 27 to 33) designed to give a detailed view of the management levels of the respondents, industrial classification of the organizations and also the employee numbers and turnover for each of the organizations. These questions also give an insight into the management levels that have responsibility for BCM in the respondent organizations. The information gathered in this section aids in addressing one of the research objectives namely the classification of the organizations in order to ascertain:

- The management levels of respondents;
- The status of the organization;

- The industrial sector in which the organization operates;
- The area in which the organization operates;
- The annual turnover and number of employees.

Coordination of BCM (Managerial Level)

	2004	2009
Director	14%	4%
Senior manager	54%	68%
Middle manager	26%	18%
Junior manager	6%	11%
Other	0%	0%
	100%	100%

Table 4.1: Coordination of BCM

The questionnaire was completed by the person with responsibility for BCM in each organization. As noted by Gallagher (2003) and BSI (2006), BCM is a continuing process which needs the input and commitment of senior management in order to keep it alive and in the minds of all stakeholders. The management level results give an indication of the seniority of the respondents to the surveys. The respondents are broken down into 11% from junior management, 18% middle management, 68% senior management with 4% at director level.

The results for the 2009 reveal that 90% of respondents came from middle management to director level compared to 94% in the 2004 survey. A greater percentage of senior management, 68% responded as opposed to 54% in 2004. Of particular note is the fact that the 2009 survey shows a 10% drop in those at director level responding (14% to 4%) and an increase from 6% to 11% for respondents at junior management level.

Ownership Status of Organizations

	2004	2009
Private limited company	40%	39%
Public sector	14%	11%
Partnership	0%	0%
Public limited company	46%	50%
Owner managed / Sole trader	0%	0%
Charity / not for profit/other	0%	0%
	100%	100%

Table 4.2: Ownership status of organizations

In the survey carried out in 2009, 50% of responses came from Public Limited Companies and Private Limited Companies composing the next highest group with 39%. The other 11% of replies came from companies in the Public (including mutual organization & semi-state) sectors.

By comparison, in the survey carried out in 2004, 46% of responses came from Public Limited Companies and 40% from Private Limited The other 14% of responses came from companies in the Public Sector. As expected, given the nature of the study, the 2009 survey results have a close correlation with those from the 2004 survey.

Industrial Sector

	2004	2009
Construction/Engineering	2%	7%
Utilities/Public administration/government	5%	4%
Professional/Consultancy	0%	0%
Manufacturing/Production	27%	21%
Business Services	2%	0%
Distribution/Transport	16%	11%
Retail/Wholesale	16%	7%
Education/Training	0%	0%
Banking/Insurance/Finance	23%	39%
Health	0%	0%
Leisure	4%	7%
Emergency Services	0%	0%
Other	5%	4%
	100%	100%

Table 4.3: Breakdown by Industrial sector

The main industry sectors from which responses were received were:

- Banking/Insurance/Finance 39%
- Manufacturing/Production 21%
- Distribution/Transport 11%
- Leisure, Retail/Wholesale and Construction/Engineering at 7% each

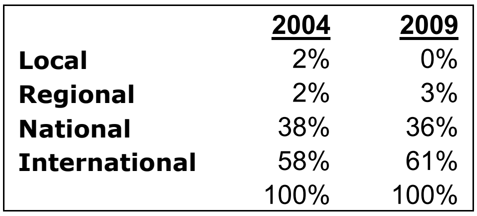
The other 8% of respondents were from: Utilities/Public, Administration /Government, Education/Training, Business Services, Emergency Services and Health sectors.

In the 2004 survey, the main industry sectors from which responses were received were:

- Manufacturing/production 27%
- Banking/insurance/finance 23%
- Distribution/transport 16%
- Retail/wholesale 16%

The other 18% of respondents were from the Leisure, Utilities/Public, Administration/Government, Construction/Engineering, Education/Training and Health sectors. In 2009 a 16% greater response was received from organizations in the Banking/insurance/finance sector.

Scope of Operation



	2004	2009
Local	2%	0%
Regional	2%	3%
National	38%	36%
International	58%	61%
	100%	100%

Table 4.4: Scope of operation

61% of survey respondents operate on an international basis with the 36% operating on a national level. The remaining 3% operate at a local or regional level. The responses give an insight into the global nature of the majority of organizations who took part in the survey. In 2004, 58% of survey respondents operated on an International basis with 38% operating on a national level. The remaining 4% operated at a local or regional level so, as expected, the results of both surveys are closely correlated.

Location

	2004	2009
Leinster	94%	89%
Munster	2%	7%
Ulster	0%	0%
Connaught	4%	4%
	100%	100%

Table 4.5: Location of organization's principal office

A total of 89% of respondents have principle offices located in Leinster, with 7% based in Munster and 4% in Connaught. In 2004 the survey had 94% of respondents having principle offices located in Leinster. These results present an indication of the cluster effect Dublin had and continues to have on the location of large organizations in Ireland.

Annual Turnover

	2004	2009
Up to €10m	0%	0%
€11m - €100m	26%	11%
€101m - €500m	34%	36%
Over €500m	40%	53%
	100%	100%

Table 4.6: Annual turnover of organizations

Analysing the responses revealed that 11% of organizations have a turnover which ranged from €11 million to €100 million, 36% have turnover in the region of €101 million to €500 million and 53% have an annual turnover of €500 million plus.

In 2004, 26% of respondent organizations had a turnover which ranged from €11 million to €100 million, 34% had turnover of €101 million to €500 million and 40% had an annual turnover of €500 million plus.

The fact that 53% of firms who responded to the 2009 survey were in the €500 million plus turnover category confirms that the survey targeted the correct organizational grouping i.e. large Irish organizations.

Number of Employees

	2004	2009
51 to 100	10%	7%
101 to 200	8%	3%
201 to 1000	36%	29%
1001 to 5000	36%	39%
5001 to 10000	4%	11%
Over 10000	6%	11%
	100%	100%

Table 4.7: Number of Employees

The sizes of the respondent organizations to this survey were as follows. 61% have more the 1000 staff with a further 29% having between 200 and 1000 staff. Looking at the survey of 2004, 46% of respondents had more than 1000 staff with a further 36% having between 201 and 1000 staff.

The European Commission (2010) define large companies as those having more than 249 employees and a turnover of €50 million or greater. The results from the questions relating to the profile of the organizations re-affirm the selection of organizations used for both the surveys as being amongst the largest in Ireland and meeting the EU definition for inclusion in this category.

4.2.2. Exploring Business Continuity Management

This section of the survey comprised a total of 19 BCM related questions designed to look at the key influences driving BCM in the respondent organizations; the level of preparedness and awareness within these organizations; and current BCM related issues and challenges facing the organizations.

The responses ascertain the attitudes and approaches taken to BCM in the respondent organizations. The research objectives addressed here include gathering information from the organizations on:

- The drivers for BCM within the organizations;
- To whom is their BCM capability communicated;
- The types of disruptive events that were experienced;
- The extend of disruption caused by certain events;
- Whether BCM plans exist;
- The extent of their BCM plans;
- Where does the responsibility for BCM lie;
- How outsourcing is handled in their BC plans;
- The sources used for gathering BCM information;
- Whether the BS25999 standard is used in forming BCM plans;
- The frequency and depth of BCM exercises undertaken;
- The status of BCM budgets.

Business Disruptions

This survey question asked respondents to characterise the extent of the disruption caused to their organization by the following events:

- Increased terrorist activity
- Power failures
- Postal strikes
- Extreme summer temperatures
- Computer viruses/bugs

The respondents were asked to rate the extent of the disruption experienced as being severe, serious, modest, non-existent or don't know. The responses to question one broke down as follows:

	2004	2009
Severe	11%	9%
Serious	26%	21%
Modest	44%	36%
Non-existent	17%	34%
Don't know	2%	0%
	100%	100%

Table 4.8: Level of Disruption Experienced

36% of responses were in the modest category, with 21% serious, 34% non-existent, 9% severe and 0% in the 'don't know' category.

	2004	2009
Increased terrorist activity	19%	8%
Power failures	41%	23%
Postal strikes	7%	15%
Extreme summer temperatures	0%	0%
Computer viruses/bugs	33%	54%
	100%	100%

Table 4.9: Events/Incidents Causing Severe Disruption.

Computer viruses/bugs were considered the largest area of severe concern for respondents at 54%. This is a reflection of the varied and ever changing attack profile faced by organizations that often rely on the internet, email and IT in order to function. At 23% power failures were the next highest in terms of causing severe disruption to respondent organizations followed by postal strikes at 15% and increased terrorist activity at 8%. Extreme summer temperatures at 0% were not an issue of severe concern for respondents.

The main differences to note between the 2004 survey and the 2009 survey are that power failures were the highest area of concern for organizations in 2004 and computer bus/viruses were the second most severe concern, these have now swapped places, based on the results of the 2009 survey. The fact that the result for postal strikes at 15% in 2009 is up from 7% on the 2004 survey is noteworthy and it is interesting to see the number of respondents who consider postal strikes as posing a severe disruption to their business even in this age of ubiquitous technology. Increased terrorist activity has dropped as a severe threat from 19% to 8%. Given that 61% of respondent organizations operate on an international basis this result is noteworthy.

	2004	2009
Increased terrorist activity	24%	7%
Power failures	22%	38%
Postal strikes	18%	14%
Extreme summer temperatures	1%	7%
Computer viruses/bugs	35%	34%
	100%	100%

Table 4.10: Events/Incidents Causing Serious Disruption.

When rating serious disruptions, power failures topped the 2009 survey at 38% with computer viruses/bugs at 34%. Postal strikes were in third place with 14% followed equally by increased terrorist activity and extreme summer temperatures at 7%.

In the 2004 survey computer viruses/bugs had the same result as 2009 at 35%. By 2009 power failures had replaced computer viruses/bugs as the most common incident causing serious disruption. Increased terrorist activity was at 24% in 2004 and was the second highest form of serious disruption; this has now dropped to 7% in 2009. Power failures were at 22% in 2004 with postal strikes at 18% and extreme summer temperatures at 1%.

	2004	2009
Increased terrorist activity	14%	22%
Power failures	18%	22%
Postal strikes	31%	28%
Extreme summer temperatures	23%	16%
Computer viruses/bugs	14%	12%
	100%	100%

Table 4.11: Events/Incidents Causing Modest Disruption.

In terms of modest disruption, postal strikes rated highest at 28%. The next highest ratings for modest disruption were power failures and increased terrorist activity jointly at 22% followed by extreme summer temperatures 16% and computer viruses/bugs 12%.

In 2004 postal strikes were also highest in the modest disruption replies at 31% with extreme summer temperatures on 23% followed by power failures 18%, computer viruses/bugs at 14% and increased terrorist activity at 14%.

	2004	2009
Increased terrorist activity	27%	32%
Power failures	11%	6%
Postal strikes	7%	13%
Extreme summer temperatures	53%	38%
Computer viruses/bugs	2%	11%
	100%	100%

Table 4.12: Non-Existent Threats to Disruption.

With a score of 38%, extreme summer temperatures were seen as a non-existent threat capable of causing disruption. The second highest non-existent threat was that of increased terrorist activity at 32%. Amongst respondents postal strikes 13%, Computer viruses/bugs 11% and power failures 6% were seen as non-existent threats.

The 2004 survey had a 53% result in favour of extreme summer temperatures as a non-existent threat, followed by increased terrorist activity at 27%, power failures 11%, postal strikes 7% and computer viruses/bugs at 2%.

	2004	2009
Increased terrorist activity	75.00%	0.00%
Power failures	0.00%	0.00%
Postal strikes	0.00%	0.00%
Extreme summer temperatures	25.00%	0.00%
Computer viruses/bugs	0.00%	0.00%
	100.00%	0.00%

Table 4.13: Don't Know.

As there were zero responses in the survey replies to this question for 2009 the results are not of import for analysis. As only four respondents proffered replies in 2004 to this question the results were also deemed not of import for analysis at that time but did show the low level of respondents who did not know what impact these events would have on their business.

Organizational BC experiences:

As noted by Burke, Wilson and Salas (2005), it is important for any survey on BCM to gain an understanding of the range of disruptive events organizations face due to the often complex environments that they operate in.

	2004	2009
Loss of site	3%	2%
Loss of telecommunications	25%	19%
Loss of IT capacity	11%	10%
Supply chain disruption	8%	7%
Loss of skills	5%	12%
Environmental liability	5%	2%
Loss of people	7%	15%
Employee health and safety scare	3%	2%
Floods/ high winds	6%	5%
Customer health/ product safety issue	3%	4%
Fire	2%	5%
Pressure group protest	4%	2%
Terrorist damage	1%	0%
Damage to corporate image/ reputation/ brand	5%	5%
Military conflict	0%	0%
Negative publicity/ coverage	12%	9%
Other	0%	1%
	100%	100%

Table 4.14: Disruption to Normal Business 2008/2009

Respondents were asked to identify the type of disruptions which they had experienced in their organizations in the previous 12 months. Loss of telecommunications at 19% was the most common incident experienced by organizations in 2009. Loss of people rated next at 15% closely followed and linked to a loss of skills at 12%. Loss of IT capacity impacted on 10% of organizations and 9% had experienced negative publicity/media coverage. A supply chain disruption caused BC issues at 7% of organizations.

Amongst other issues faced by organizations in 2009 included damage to the corporate brand, disruption related to fires and to floods/high winds – each of which were experienced by 5% of respondents. Customer health/product safety issues garnered a 4% response with environmental liability, loss of site, employee health and safety scare and pressure group protests each causing disruption to 2% of respondent organizations. The "other" category at 1% included a gas leak. None of the respondents experience disruption related to terrorist damage or military conflicts.

In the 2004 survey loss of telecommunications had impacted on 25% of organizations, 6% more than 2009. The 2004 revealed that negative publicity/coverage had caused BC issues at 12% of respondent organizations and this had dropped by 3% to 9% in the 2009 survey. Loss of IT capacity was reported by 11% of organizations in 2004 and 10% in 2009 and so remains at a similar level. Results for supply chain disruption also were similar in both surveys, in 2004 8% of respondents had suffered some supply chain disruption in the past year and in 2009 the figure was 7%. In 2009 loss of people and loss of skills at 15% and 12% respectively had increased from the 2004 survey results of 7% and 5%.

In 2004 other impacts suffered by companies were in the areas of floods/high winds at 6%, pressure group protests 4%, loss of site 3%, employee health scares 3%, customer health/product safety issues 3%, damage to corporate image 5% and fire at 2%. Similar low results were apparent in the 2009 survey. In both surveys military conflict rated at 0%.

The Importance of Business Continuity to Management

	2004	2009
Very important	58%	56%
Important	32%	30%
Neutral	8%	11%
Not important	2%	3%
Not at all important	0%	0%
Don't know	0%	0%
	100%	100%

Table 4.15: The importance of business continuity to senior management

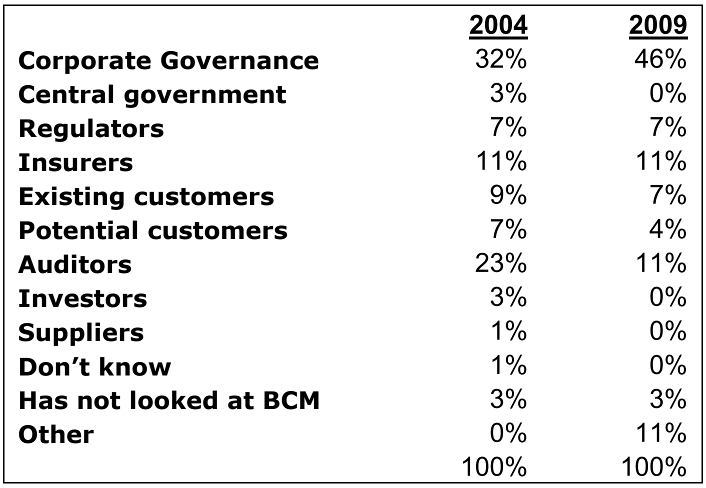
As identified by Seow (2009), not getting top management buy in and commitment to starting and sustaining a BCM programme in an organization can be an obstacle to the programme's success.

Business continuity was considered either very important 56% or important 30% by the majority of responding organizations. That 14% of respondent firms rated the importance of business continuity to senior management as either neutral 11% or not important 3% is noteworthy and indicates that for some organizations BC is still not of high strategic importance. In 2004, 90% of respondents had rated business continuity as either very important 58% or important 32%. This combined result has dropped by 4% in 2009.

In the 2004 survey 10% of respondents rated business continuity as either neutral (8%) or not important (2%). This response has risen to a combined 14% in 2009. As only large organizations were surveyed this 14% result is considered high and has risen by 4% from 2004.

BCM Organizational Drivers for Change

The impact on organizations of corporate governance and regulation is well noted in the literature as a BCM driver for change by Elliott, Swartz and Herbane (2010), O'Hehir (2007), Dye and Langsett (2008).



	2004	2009
Corporate Governance	32%	46%
Central government	3%	0%
Regulators	7%	7%
Insurers	11%	11%
Existing customers	9%	7%
Potential customers	7%	4%
Auditors	23%	11%
Investors	3%	0%
Suppliers	1%	0%
Don't know	1%	0%
Has not looked at BCM	3%	3%
Other	0%	11%
	100%	100%

Table 4.16: Key drivers for change

Clearly the main driver for organizations changing their approach to BCM was corporate governance at 46%. The next highest responses were, at 11% each, insurers, auditors and "other". Regulators and existing customers were considered as key drivers of change by 7% with 3% of respondents declaring that they had not "looked" at BCM Finally, 4% of respondents cited potential customers as a driver for having changed their approach to BCM.

Comparing the 2004 and 2009 survey results shows that corporate governance has risen by 14% from 32% in 2004 as the main driver of BCM activity. Auditors have become less significant drivers at 11%, down 12% from 23% in 2004. Insurers have stayed static at 11% as have the regulators at 7%. The existing customer category is down 2% from 9% in 2004 to 7% in 2009 with potential customers falling to 4% from 7%. Those respondents who have not looked at BCM are the same in both surveys at 3%. The other category was not included in the 2004 survey but was included to capture other drivers in the 2009 survey and consisted of best practice and technology refresh.

Providing Evidence of BCM

	2004	2009
Central government	7%	3%
Insurers	15%	16%
Regulators	12%	13%
Banks	5%	3%
Other external funding bodies	1%	0%
Potential customers	5%	15%
Existing customers	5%	11%
Auditors	35%	33%
Credit rating agencies	1%	2%
No external requests	14%	4%
Other	0%	0%
	100%	100%

Table 4.17: Providing evidence of BCM

At 33% auditors were the main group asking respondent organizations for evidence of BCM. Insurers were next at 16% closely followed by potential customers at 15% with regulators at 13% and existing customers at 11%. No external requests stands at 4% and next with single digit percentages, come banks, and central government at 3% with credit rating agencies at 2%.

Comparing the 2004 and 2009 surveys one finds that auditors still remain the main group asking for evidence of BCM. Auditors stood at 35% in 2004 compared to 33% in 2009. Insurers at 15% have risen slightly in 2009 to 16%.

The major change between surveys is that in 2004, 14% of respondents had not as yet received requests for evidence of BCM from any of the bodies or groups. This result has shown a drop to 4% in the 2009 survey and shows that more requests are being made for evidence of BCM from external sources.

Requests from central government have dropped from 7% in 2004 to 3% in 2009. This drop should be noted as government should include the private sector when dealing with civil emergencies according to Somers and Svara (2009). Existing customers and potential customers at 5% in 2004 have risen to 11% and 15% respectively in the 2009 survey showing a greater level of interest from customers who want to ensure that supplier organizations have BCM in place. Scoring 5%

in 2004, banks scored 3% in the 2009 survey. Credit rating agency requests for evidence of BCM remains similar between surveys at 1% in 2004 compared to 2% in 2009.

BCM Information Sources

Respondents listed the following as sources of guidance and knowledge: the Business Continuity Institute (BCI); trade; peers; the internet; external vendors; internal resources; industry contacts; insurers; partners; consultants; auditors; Sabane Oxley; the IT Department; attendance at seminars and workshops and, finally, group head/corporate offices;

As can be seen from the above list organizational BCM information comes from a wide variety of resources. No one body/entity appeared more than others in the survey. It is also noteworthy that respondents did not identify the British Standards Institute (BSI) as a source of information on BCM. These results are similar to those of the 2004 survey.

Business Continuity Plans.

	2004	2009
Yes	90%	89%
No	8%	7%
Don't know	2%	4%
	100%	100%

Table 4.18: Does your organization have a Business Continuity Plan?

The main results to note in response to this question is that 7% of respondents do not have a business continuity plan and also 4% did not know whether their organization had a business continuity plan. 89% of respondent organizations had a BC plan in place. The results from the 2009 survey are comparable to those of the 2004 survey where 8% of respondents did not have a BC plan and 2% did not know if their organization possessed a BC plan. In 2004 90% of organizations indicated that they had a BC plan, this dropped to 1% to 89% in 2009

Business Continuity Plan Coverage

	2004	2009
Loss of site	11%	11%
Loss of IT capacity	14%	13%
Loss of skills	5%	5%
Loss of people	5%	7%
Floods/ high winds	6%	4%
Fire	9%	9%
Terrorist damage	6%	5%
Military conflict	4%	2%
Loss of telecommunications	14%	12%
Supply chain disruption	5%	7%
Environmental liability	3%	4%
Employee health and safety scare	5%	7%
Customer health/ product safety issue	2%	3%
Pressure group protest	3%	2%
Damage to corporate image/ reputation/ brand	4%	5%
Negative publicity/ coverage	4%	4%
	100%	100%

Table 4.19: What was covered by Business Continuity Plans?

While BCM research as conducted by Herbane (2010) currently emphasises, IT should not be the central focus of BCM but is just a part, the two highest results were as follows, loss of IT capacity 13% and loss of telecommunications 12%. These are followed by loss of site 11% and fire at 9%. Supply chain disruption, employee health and safety scare and loss of people each scored 7%. Next were loss of skills, terrorist damage and damage to corporate image/reputation/brand at 5%, floods/high winds, negative publicity/coverage and environmental liability at 4% and customer health/product safety issue at 3%, military conflict and pressure group protests at 2%.

In the 2004 survey the most commonly covered disruptions were loss of IT capacity and loss of Telecommunications – both at 14%. Loss of site at 11% and fire at 9% showed exactly the same result in both surveys. Supply chain disruption scored 5% in 2004 and this has risen to 7% in the 2009 survey showing the growing importance of supply chains to organizations. Loss of people has also risen from 5% to 7% in 2009. Loss of skills remained at 5% in both surveys with terrorist damage dropping from 6% to 5% in the 2009 survey. Floods/high winds have dropped 2% in 2009 from 6% in the 2004 survey to 4%. Employee health and safety scares were included in 5% of plans in 2004 this figure now stands at 7%. Military conflict has dropped to 2% in 2009 from 4% in the 2004 survey and damage to the corporate image/reputation/brand, which stood at 4% in 2004 rises slightly to 5% in 2009. Negative publicity/coverage, remained the same in both surveys at 4%. In 2004 pressure group protests were covered by 3% of plans; this was down to 2% for 2009. Environmental liability was included in the plans of 3% of respondents in 2004 compared with 4% in 2009. Finally, customer health/product safety rose from 2% in 2004 to 3% in 2009. Overall, these results could be judged as remaining relatively stable between surveys.

Exercising the BCP

As noted by The Standard, Gallagher (2003), Alexander (2005) and Bradbury (2008), it is important that the BC plans are subject to regular review, exercising and updating and that all areas of the organization are covered including the plans, the process, the people, and the infrastructure. Alexander (2005) advises that plans should be tested and updated periodically on a repetitive cycle.

	2004	2009
At least every 3 months	7%	0%
At least every 6 months	26%	28%
About once a year	36%	64%
About every 2 years	20%	8%
About every 3 years	0%	0%
Not at all	11%	0%
	100%	100%

Table 4.20: Frequency with which Business Continuity Plans were exercised

The main statistic to highlight is that 64% of respondents rehearse BC plans about once a year; 28% rehearse at least every 6 months and 8% exercise about every 2 years. There were no replies in the not at all or about every 3 years categories in the 2009 survey.

The 2004 survey results showed that 11% of organizations did not exercise their BCPs which perhaps match the 10% of respondents who did not know whether or not they had a BC plan in place. This figure dropped to 0% for the 2009 survey.

The percentage of respondents exercising their plan at least once a year has risen from 36% to 64%: with those exercising at least every 6 months standing at 28% in 2009 against 26% in the 2004 survey. In 2004 7% of respondents reported that they rehearse their BCPs every 3 months, this has dropped to 0% in the current survey. 20% of respondents in 2004 exercised their BCP about every 2 years; this result dropped to 8% in 2009.

Outcome of Exercises

	2004	2009
Yes, but not addressed	12%	8%
Yes, have been addressed	71%	84%
No	12%	4%
Don't know	5%	4%
	100%	100%

Table 4.21: Has a Business Continuity plan exercise revealed any shortcomings in its effectiveness, and have these been addressed?

84% of respondents said that once issues had arisen during BCP exercises they had been addressed. At 8% some organizations have identified shortcomings in BC arrangements during exercises but these have, as yet, not been addressed. The fact that 8% of respondents answered either "no" or "don't know" to this question may lead one to question the seriousness with which BCM/BCM exercises are treated within some organizations.

In the 2004 survey, 71% of respondents said that once issues had arisen during BCP exercises they had been addressed. This result has risen 13% to 84% for the 2009 survey. 17% of respondents answered "no" (12%) or "don't know" (5%) in 2004. The 2009 results showed a drop of 9% to 8% for the combined "no" and "don't know" responses.

Scope of Exercises

	2004	2009
IT recovery	42%	16%
Workplace recovery	14%	28%
Business unit	19%	20%
Organization-wide	14%	24%
Board level scenario	6%	8%
Don't know	5%	4%
	100%	100%

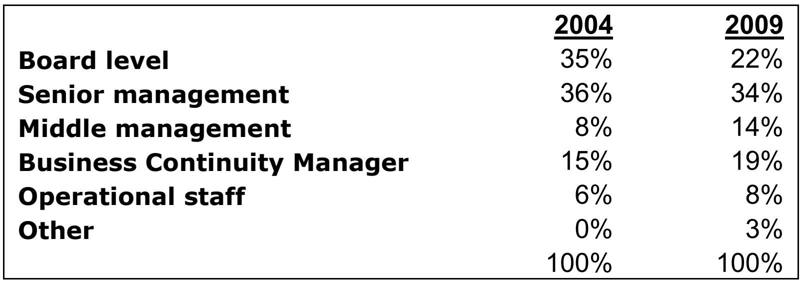
Table 4.22: Scope of Exercises.

As outlined in the table above, 28% of respondents extend BCP exercising to workplace recovery level. Organization wide plan exercising is completed by 24% of respondent organizations. Business unit level exercises are completed in 20% of organizations with 16% of organizations covering only IT systems recovery. 8% of respondent organizations exercise their BCPs with board level scenarios and 4% responded that they did not know to what level their BCPs were exercised.

The 2004 survey revealed that 42% of exercises extended only as far as IT recovery: this figure has dropped to 16%. Business unit exercises were completed by 19% of respondents in 2004 compared to 20% in the 2009 survey. Workplace recovery exercises stood at 14% in 2004 and doubled to 28% in 2009 while organization wide rehearsals which were at 14% in 2004 and increased to 24% in 2009. These results show that there is some movement away from having a purely IT focus when exercising BC plans.

Responsibility for BCM

Respondents were asked to identify who had responsibility for Business Continuity Management; who was involved in creating the Business Continuity Plan and who was the owner of the plan and, therefore, responsible for effective implementation. The literature clearly states that those responsible need to have the required levels of authority and seniority in order to make the BCM programme successful.



	2004	2009
Board level	35%	22%
Senior management	36%	34%
Middle management	8%	14%
Business Continuity Manager	15%	19%
Operational staff	6%	8%
Other	0%	3%
	100%	100%

Table 4.23: Responsibility for Business Continuity Management

Survey responses revealed that in 34% of the organizations surveyed senior management were responsible for BCM and 22% reported that responsibility rested at board level. 19% of respondents have a specific business continuity manager; 14% of respondents placed responsibility for BCM at middle management level; 8% of respondents have operational staff responsible for BCM and, finally, 3% placed responsibility with "other" staff (IT and various other departments). This is an important finding as numerous references to the importance of senior management participation and backing are to be found in the literature as noted by Barnes (2001), Elliott, Swartz and Herbane (2010), Gallagher (2003), Koch (2004) and Seow (2009).

In the 2004 survey 36% of responses placed responsibility at senior management level, this has dropped 2% in the 2009 survey. Board level responsibility was at 35% in 2004. This has dropped to 22% in 2009. The percentage with specialist business continuity managers taking responsibility for this area of the business rose from 15% in 2004 to 19% for 2009. Middle management was responsible in 8% of organizations in 2004 compared to 14% in 2009. Finally, operational staff at 6% in 2004 now stands at 8% in 2009. In the 2004 survey no responses were recorded in the "other" category. Perhaps most worthy of note is the 13% drop in those reporting that responsibility for BCM sat at board level. On a more positive note, this drop has been offset by an increase in specific business continuity managers.

	2004	2009
Board level	3%	0%
Senior management	25%	20%
Middle management	30%	32%
Business Continuity Manager	26%	33%
Operational staff	16%	15%
Other	0%	0%
	100%	100%

Table 4.24: Level of staff involved in creating the Business Continuity Plan

In 33% of respondent organizations the business continuity manager and at 32% middle management have the main involvement in creating the BC plan with senior management at 20% and operational staff's involvement standing at 15%.

The 2004 survey results show that middle management involvement stood at 30%, 2% less than in 2009. In the 2004 survey business continuity manager involvement was at 26%, this has risen to 33%. Senior management involvement was at 25% in 2004 and this result is down 5% to 20% for 2009. Operational staff rated 16% in 2004 and this has dropped 1% in 2009 to 15%. The level of board involvement has dropped from 3% in 2004 to no involvement in 2009.

It should be noted that the responsibility for BC plan creation has moved more from senior management to middle management and specific business continuity management between surveys.

	2004	2009
Board level	10%	7%
Senior management	35%	46%
Middle management	24%	11%
Business Continuity Manager	20%	22%
Operational staff	11%	14%
Other	0%	0%
	100%	100%

Table 4.25: Level at which plan ownership and implementation sits.

In the 2009 survey, plan ownership and responsibility for implementation sat at senior management level in 46% of organizations. In 22% of respondent organizations the business continuity manager is the plan owner with operational staff at 14%, middle management at 11% and board level at 7%. As noted by Brazeau (2008) it is important that everyone in the organization embraces BCM and the results above show that whilst senior management have the main share of responsibility, it is also spread across other organizational levels.

A comparison of results shows that the main areas of change has been an 11% increase in plan ownership by senior management and a 13% decrease in those at middle management levels having ownership of the BC plan. Ownership by a specialist business continuity manager is up slightly from 20% in 2004 to 22% in 2009. Operational staff were seen as plan owners in 11% of organizations in 2004 compared to 14% in 2009. Finally, board level plan ownership has dropped from 10% in 2004 to 7% in 2009.

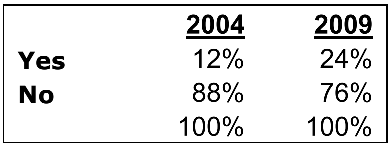
BS25999

	2004	2009
Yes	55%	68%
No	45%	32%
	100%	100%

Table 4.26: Familiarity with the BS 25999

The 2009 survey results show that 68% of respondents were familiar with the BS25999 British standard for BCM and 32% were not familiar with The Standard. As BS25999 was not created until 2006/2007 the original 2004 survey asked a question regarding familiarity with the Publicly Available Specification (PAS) 56 initiative for BCM that was released in 2003. Many consider it the fore runner of BS25999. By 2004 55% of respondents were aware of PAS 56 with 45% not being aware of the specification. In 2004 the level of response showed that more work needed to be done on communication and raising awareness of the specification. With not having a single agreed international BCM standard this situation is likely to persist into the foreseeable future.

Use of BS25999



	2004	2009
Yes	12%	24%
No	88%	76%
	100%	100%

Table 4.27: Does your organization use BS 25999?

As BS25999 is the main standard used for BCM it is noteworthy that 76% of respondents to the 2009 survey said that they did not use BS25999 in their organization; with 24% saying that they did. From a communications perspective this is a stark result given that the survey was completed by those with BCM responsibility in their organizations. The response indicates that BS25999 has not as yet had a wide impact on respondent organizations.

In 2004 a similar question was asked regarding Publicly Available Specification (PAS) 56 initiative for BCM. The results were that only 12% of respondents had used PAS 56 with 88% not using it.

Communicating Business Continuity Capabilities

As noted from the literature, The Standard, Barnes (2001), Elliott, Swartz and Herbane (2010) and Gallagher (2003) outlined that communicating the importance of the BCM programme to the whole organization and appropriate stakeholders is vital in order to keep it in focus.

	2004	2009
Regulators	13%	11%
The investment community	3%	3%
Insurance companies	13%	13%
Shareholders	9%	4%
Senior management / Board	33%	29%
Employees	17%	20%
Local community	1%	1%
Suppliers	4%	7%
Customers	2%	7%
Don’t know	2%	0%
Other *(please specify)*	3%	5%
	100%	100%

Table 4.28: Organizations to which Business Continuity capability has been communicated

The 2009 survey results revealed that it was to senior management/the board (29%) that organizational BC capabilities were most likely to be communicated. This was followed by: employees at 20%; insurance companies at 13%; regulators at 11%; customers and suppliers 7%; “other” (which included auditors and the parent company) 5%; shareholders 4%; investment community 3%; and the local community 1%.

A comparison of the 2009 and the 2004 results shows that while the percentages have altered the rankings have not changed greatly with senior management the highest grouping at 33%, employees at 17%, insurance companies 13%, regulators 13%, then shareholders 9%, suppliers 4%, investment community 3%, customers and don’t know at 2% and the local community at 1%. In 2004, under the “other” category, 3% of respondents identified three other parties to whom BC capability was communicated. These included Head Office (in the case of multinationals with Irish offices), audit departments (again an internal entity) and emergency personnel (but this was in relation to a major government run authority’s response). The response to the “other” category has risen to 5% for the 2009 survey and consists of auditors and parent company. A further point to note is that despite the drive to make companies more community aware in order to be better corporate citizens, only 1% of respondents to both surveys communicated the organizations BC capability to the local community.

What is Covered in Business Continuity Plans

The literature, The Standard and Rossing (2007), emphasises that it is important to understand the organization by identifying its main products and services and the resources and activities that support them in order to ensure the organization is a going concern. It is therefore vital that all areas are covered by BC plans.

	2004	2009
Production/ manufacturing	7%	6%
Finance	10%	12%
Sales	8%	10%
Marketing	7%	5%
Purchasing	8%	8%
Outsourcing	4%	6%
Human resources	10%	11%
Information technology	17%	14%
Facilities management	12%	12%
Security	9%	9%
Public relations	8%	6%
Other *(please specify)*	0%	1%
	100%	100%

Table 4.29: Departments included in Business Continuity Plans

At 14%, the information technology function was most likely to be included in the BCP. This was followed by facilities management and finance (both at 12%). Human Resources were included in 11% of plans, sales in 10%; security in 9%, purchasing in 8%, public relations, production/manufacturing and outsourcing in 6%, and the marketing department in 5% of plans. In the "other" category (1%) respondents identified administration and client services as other Departments that are included in their organizational BC Plans.

When comparing the 2009 survey results to the 2004 survey the results revealed that security, facilities management and purchasing remained unchanged and there was a swing of just 1% for the inclusion of, production/manufacturing and human resources. Information technology had a 3% reduction between surveys with public relations, outsourcing and sales showing 2% shifts. In the "other" category in 2004 less than 1% (0.4%) of respondents identified, business and operational units, retail, operations, logistics, category management and telecommunications as other areas that are included in the organizational BCP.

Outsourcing

Outsourcing of non-core functions and services according to Gallagher (2003), present BCM with a particular set of problems in that control for the outsourced function or service now resides with a third party. It is therefore important to gain an understanding of the levels of outsourcing used in organizations and how BCM is handled.

	2004	2009
Yes	68%	81%
No	20%	19%
Not applicable	12%	0%
	100%	100%

Table 4.30: Outsourcing of facilities/services?

Outsourcing is used by 81% of respondents with the remaining 19% saying that they did not outsource any facilities/services. Between surveys there has been a major change with 68% saying they used outsourcing in 2004 increasing by 13% in 2009. There were 0% results for 2009 in the not applicable category.

	2004	2009
Yes	52%	67%
No	20%	33%
Not applicable	28%	0%
	100%	100%

Table 4.31: Requirement for outsource suppliers to have a BCP

In 2009 67% of those who used outsourced facilities/services reported that their outsourcing partners were required to have BC plans. 33% said they did not have this requirement. This shows a rise of 15% from 2004 when 52% of respondents who outsourced facilities/ services stated that they required their outsourcing partners to have BC plans. In 2004 20% of respondents said they did not have such a requirement in place, this has risen to 33% in 2009. There was a 0% result in 2009 in the not applicable category.

	2004	2009
Statement from suppliers	52%	58%
Examination of Business Continuity Plans	29%	26%
Involvement in rehearsals	12%	16%
Involvement in Business Continuity development	7%	0%
	100%	100%

Table 4.32: Verification of outsource suppliers BCPs

Statements from suppliers, at 58%, were the most popular method of verification used by organizations to ensure outsource suppliers had BC plans in place in 2009. 26% of respondents actually examined their outsourcing partners BC plans and 16% actually involved providers of outsourced facilities/services in BCM rehearsals. None of the respondents to the 2009 survey were involved in the development of the BC plans of outsourcing partners.

In the 2004 survey 52% of respondents relied on a statement from the outsourcing supplier to verify their BC plans. 29% actually examined their outsourcing partners BC plans and 12% of respondents took part in rehearsals with partners. 7% were involved in the development of the BC plans of outsourcing partners in 2004. Results between surveys have remained broadly similar apart from a 7% decrease in the involvement in business continuity development.

Business Continuity Budgets

Increase substantially	8%
Increase marginally	23%
Remain the same	65%
Decrease	4%
Don't know	0%
	100%

Table 4.33: Business Continuity Management budgets

A total of 65% of respondents said that their BCM budget would remain the same for 2009. An interesting finding, given the current economic climate, was that 8% of respondents said that their BCM budgets would increase substantially and 23% reported that their BCM budgets would increase marginally in 2009. Only

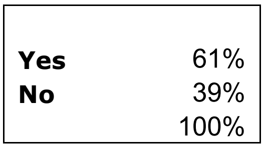
4% said their BCM budget would decrease. This question was added into the 2009 survey so no comparison against the 2004 survey was possible.

4.2.3. Power Management

This section of the survey comprised a total of five questions designed to look at how organizations deal with power supply issues and how/if they assess the power readiness of their supply chain partners. This section was added to the 2009 survey because it was identified as the area of most severe concern in the 2004 study. The goal of this section of the survey is to answer the research objectives to review how the respondents specifically handle power issues. Included here is the gathering of information on:

- Their experience of power outages;
- Whether power issues are covered in BC plans;
- The extent of generator and UPS use;
- The extent of generator and UPS use amongst the respondents outsource suppliers.

Power Issues

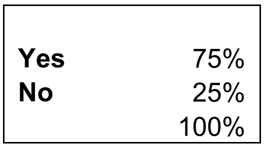


Yes	61%
No	39%
	100%

Table 4.34: Has your organization experienced any power outages in the past year?

Power outages affected 61% of respondent organizations in the previous year. In order to cope with this level of power instability the following questions were asked to gain a better understanding of what organizations were doing to mitigate this risk.

Power Coverage in BCP



Yes	75%
No	25%
	100%

Table 4.35: Does your Business Continuity Plan cover power outages specifically?

Power outages were covered by 75% of respondent's BC plans. 25% did not cover this issue in their BC plan.

Generator Ownership

Yes	86%
No	14%
	100%

Table 4.36: Does your organization have its own generator?

A total of 86% of respondent organizations have their own generators. This result may partially account for the result in Table 4.35, where 25% of respondents do not have power issues covered in their BCP. Perhaps they consider they have enough protection from power outages with their generator backup.

UPS Ownership

Yes	96%
No	4%
	100%

Table 4.37: Does your organization have its own Uninterrupted Power Supply (UPS)?

With 96% of respondents having their own Uninterrupted Power Supply (UPS) systems, nearly all organizations are covered against power outages for a time at least. The UPS systems allow organizations to gradually shut down non-essential computer and telephone systems and to maintain critical systems for as long as the UPS allows or until power supplies are restored. As the majority of power outages experienced are short in nature UPS systems can often take on the crucial load for organizations. UPS systems also provide cover for any time lags whilst generators power up during power outages.

Verifying Outsourcers Power Capability

Statement from suppliers	64%
Examination of Business Continuity Plans	28%
Involvement in rehearsals	8%
Involvement in Business Continuity plan development	0%
	100%

Table 4.38: Do your outsource suppliers have generators & UPS capabilities to ensure their services, and if so how do you verify that they do?

To find out if outsource suppliers have generators and UPS capabilities, 64% of respondents relied on a statement from the outsourcing supplier to verify their generator and UPS capabilities, 28% examined their outsourcing partners BC plan and, 8% took part in rehearsals with partners. None of the respondents were involved in the development of the BC plans of outsourcing partners in order to ensure they had adequate generator and UPS capabilities.

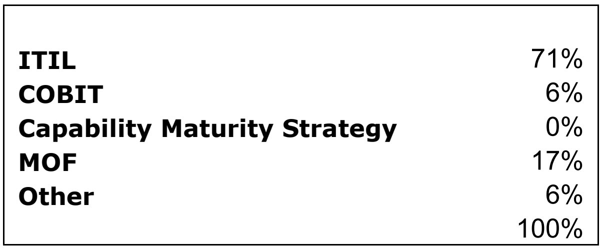
4.2.4. Information Technology Service Management (ITSM)

This section of the survey comprised a total of three Information Technology Service Management (ITSM) related questions designed to look at the spread of this initiative across organizations. These questions were not asked in the 2004 survey.

In the past IT was mainly internally focused and concentrated on technical issues. Today, businesses have high expectations about the quality of services delivered by IT and these expectations change with time. For IT departments to live up to business expectations they need to focus on service quality and customer oriented approaches and a more business like attitude to the provision of service. Service Management (SM) frameworks focus on providing high quality services with a primary focus on customer relationships. This means that IT departments should have a strong relationship with its customers and partners often with agreed Service Level Agreements (SLAs) between them. SM, given its service delivery orientation, has a BCM component and is of import in maintaining applications in organizations. SM therefore has a bearing in any study relating to BCM and so it was included in this survey in order to get a view of its importance to large Irish organizations.

The goal of this section of the survey is to answer the following research objective: Evaluate the use of Information Technology Service Management (ITSM) within the organizations. The main ITSM approaches used in organisations are the Information Technology Infrastructure Library (ITIL), the COBIT framework for IT Governance and Control, Capability Maturity models/strategies a process improvement approach whose goal is to help organizations improve their performance and the Microsoft Operations Framework (MOF) which provides guidance for IT practices and activities, helping to establish and implement reliable, cost-effective IT services.

ITSM Approaches



ITIL	71%
COBIT	6%
Capability Maturity Strategy	0%
MOF	17%
Other	6%
	100%

Table 4.39: ITSM Approaches Followed.

71% of respondents said that they follow the ITIL standard. This is the lead standard in Europe in the area of ITSM. Development started in the late 1980s and since that time ITIL has become one of the leading standards in ITSM. Starting as a guide for the UK government, the British Standards Institute published a Code of Practice for IT Service Management (PD0005) which was based on the principles of ITIL. There is now a full standard, BS15000.

The fact that 17% of respondents use MOF is another indication of the importance of ITSM as MOF is primarily based on ITIL. A further 6% of respondents either use COBIT or another ITSM framework.

Various ITSM software tools are used across the IT industry to provide views on ITSM. Amongst the tools used are Microsoft's Systems Centre Operations Manager (SCOM), Hewlett Packards Openview software which contains network and systems management products, BMC's Patrol software used to monitor multiple IT environments and components, IBM's Tivoli integrated service management software and Computer Associates (CA) Unicentre technology management software suite.

Use of ITSM Tools

MS SCOM	26%
HP Openview	23%
BMC Patrol	14%
IBM Tivoli	23%
CA Unicentre	14%
Others	0%
	100%

Table 4.40: Use of ITSM tools

The results show Microsoft SCOM/SCOM, HP Openview and IBM Tivoli are particularly popular ITSM tools used by respondents.

Drivers for Implementing ITSM

Improve service levels for the business	25%
Improve IT Internal processes	58%
Reduce the costs of service provision	13%
Other	4%
	100%

Table 4.41: Drivers for Implementing ITSM

The pervading driver in organizations considering ITSM implementation was to improve internal IT processes at 58%. This is one of the main goals for ITSM initiatives. At 25%, improving service levels to the business is next followed by reducing the costs of service provision at 13%. The low result for improving service levels to the business shows that in many organizations ITSM, as is the case with BCM, is largely driven from an IT perspective.

4.2.5. Conclusions

The next stage of the research process involves exploring in greater depth some of the themes identified in the survey results using interviews with industry experts. This issue will be tackled in Chapter five of this research.

CHAPTER FIVE

INTERVIEWS

5.1 Introduction

According to Bell (2005):

> "Moser & Aron (1972) describe the survey interview as 'a conversation between interviewer and respondent with the purpose of eliciting certain information from the respondent." (Bell 2005 p. 157)

Following on from the survey and in order to explore some of the themes further it was decided to undertake a number of semi-structured interviews with BCM industry experts. The seven semi-structured interviews undertaken were based around a series of twenty one questions (see Appendix B) derived from the main themes found in the survey as outlined in Chapter Four. The interviews therefore acted as a crosscheck of the survey findings.

This chapter outlines the results of the interviews that were conducted with seven experts working in the area of BCM in Ireland. These experts represented the foremost authorities in the area of BCM practice ranging from BCM consultants and practitioners, to providers and members of the professional bodies - the Business Continuity Institute and the Emergency Planning Society.

As outlined in Chapter Three the responses to the interview questions were coded according to a number of themes.

These included:

- Where does responsibility for BCM sit in organizations;
- Is BCM a high priority for senior management;
- The incidents/events that trigger BCM;
- The vulnerability of organizations to specific events;
- The lower perceived threat from terrorist activity;
- The impact of improved organizational business processes and the impact on resilience;
- The organizational investments made in BCM;
- The role of central government in the BCM capabilities of organizations;

- The role of regulators in the BCM capabilities of organizations;
- Where do organizations get their information on BCM;
- Are government agencies used as a source of BCM information;
- Within organizations, who is responsible for BCM, involved in creating the Business Continuity Plan and owns/implements the plan;
- The impact of BS25999 on large organizations;
- To whom do organizations communicate their BC capabilities;
- How do organizations deal with outsourcing in a BCM context;
- How do large organizations handle power issues;
- Is IT and communications still the main focus of BCM;
- The frequency with which organizations exercise their BC plans;
- What could be done to increase the uptake in BCM in large Irish organizations.

The coded material was then grouped together so that a general answer to the questions could be gleaned. Any major variations in interview responses are highlighted in the write up.

5.2 Interview Analysis

In the organizations which I have studied responsibility for BCM seems not to sit at Director Level. Does this match your view of BCM?

The response from those interviewed reflected the results which emerged from the survey and also from the literature review as noted by Gallagher (2003) and BSI (2006). Whilst one respondent said that they thought responsibility was much more of a board issue today, than in the past, even they added a caveat saying that "responsibility for actual implementation was not at board level" and that "board level input was mainly to act as a sponsor for the BCM programme with responsibility delegated to other levels in the organization".

Respondents indicated that BCM had grown through IT and finance departments and was driven by audit. Directors do not seem to look at continuity risks as a direct responsibility. It was felt that this is due to the immaturity of BCM in many organizations. Other responses indicated that whilst it was purely an IT responsibility in the past, a move into operational units has been witnessed in more recent times. Some expressed the view that often BCM does not arise at a senior management level and was largely tasked to middle management within organizations. The view that directors and senior managers view BCM as "a necessary evil" was prevalent. Only when an incident occurs and the response is haphazard do directors and senior management take an active interest in BCM.

An interesting dimension which emerged in response to this question was that "directors not having responsibility for BCM is not necessarily a bad thing". It was felt that responsibility for BCM should flow up through the organization with departmental managers having ultimate responsibility and reporting up through the organization to board level. If the board, or a member of the board, was to have BCM responsibility then it should be from an overarching/strategic organizational risk perspective.

Overall the experience of interviewees reflected the view that BCM is delegated to upper middle management in IT, operational and risk departments.

Is BCM a high priority for senior management?

Responses ranged from a blunt "No" to the fact that it "depends on the sector in which the organization operates". It was felt that financial, pharmaceutical and multinational organizations usually took BCM seriously whereas less regulated and indigenous Irish organizations were less likely to have it as a high priority. BCM was seen as being "a priority for organizations but it is often moved down the list" as other priorities take precedence. Where organizations were forced to look at BCM by regulation it had a high priority. "If senior management had a choice they would forget about it" and "rarely is it embraced by them because BCM is not seen as a product that is tangible" and it "is seen as a cost that can be avoided". Organizations do not "see anything visible by doing BCM" so it is therefore "not driven by senior management unless it is a crucial requirement for their business" e.g. in the financial, pharmaceutical or food production sectors. One interviewee commented that in recent times "suppliers were more likely to be asked for reassurance of supply by their customers" but again this was often sector dependent.

What would you say are the incidents most likely to disrupt an organization and trigger the need for BCM?

As noted by Burke, Wilson and Salas (2005), it is important for any survey on BCM to gain an understanding of the range of disruptive events organizations face due to the often complex environments that they operate in. The main issues identified as triggers for BCM, according to those interviewed, were IT related issues, including communications and system related problems. Utility supply, incidents related to leaks/water damage and supply chain problems were also mentioned as incidents most likely to disrupt an organization. It was felt that IT issues such as loss of key systems, services and infrastructure presented the most obvious need for BCM as they can have the largest, most visible impact on an organization.

Other responses of note were that "a full blown building incident is rare" and that recently "the implementation of unified communications infrastructures having the telephone and IT networks linked together had caused some BCM issues". The issue of people, especially in relation to the impact of pandemics, and "deliberate, malicious crime incidents" were also mentioned as BCM triggers.

Why do you think organizations are vulnerable in these areas?

- **Loss of telecommunications**
- **Loss of people**
- **Loss of skills**
- **Loss of IT capacity**

Interviewees all noted that loss of IT capacity and telecoms were considered areas of vulnerability as they are one of the "most visible" elements of an organization and they are core services for nearly all large organizations today. Organizations are vulnerable in these areas due to the fact that "not enough resilience has been built into infrastructures" and also the fact that in Ireland there are a "limited set of suppliers from a telecoms perspective". It was noted that "few organizations have telecommunications resilience strategies" either because they physically cannot have them (for example in the case of single access points to buildings) and so have single points of failure in their networks or the fact that it is too costly to have redundant/backup telecommunications links in place. It was mentioned that the telecommunications infrastructure in Ireland was now "more robust than had been the case in the past". Often only when an incident effects them do some organizations look at their IT and telecommunications BCM strategies.

When addressing the loss of skills and loss of people, interviewees mentioned that there are various processes and initiatives in place in most large organizations, particularly those in the financial sector, to address these issues. These initiatives and processes include "cross training", "succession planning" and "buying in skills cover by outsourcing to 3rd parties who can provide coverage for skills shortages". The recent, recession-based, redundancy drive was noted as a major cause of loss of people and skills as it is usually the older more experienced staff that were targeted in these initiatives. It was noted that "often experienced staff that have been made redundant are subsequently brought back into the organization on contract to cover the skills shortage". Loss of people and skills were highlighted in one response, as being "the biggest risk to organizations at the present time, as experienced staff was feeling undervalued due to the current economic climate and the ensuing promotion and wage/bonus restrictions that have resulted".

My study revealed that the perceived threat from terrorist activity has dropped over the past 5 years – why do you think this is so?

The Northern Ireland Peace Process was noted in all interviews as being a major contributory factor to the drop in the perceived threat from terrorism in Irish organizations. It was also noted that where organizations operated on a UK or on a global basis that the terrorist threat perception would probably be higher. The point was made that "the threat from terrorism had actually dropped in Ireland", that "there were fewer headline terrorist incidents such as 9/11" and that these all "contributed to the threat perception levels being lowered". It was stated that “the media have a large role to play in the perception of threats levels in organizations” and that the “Irish media coverage of terrorist threats in Ireland over recent times is low”. “The threat from terrorism, as acknowledged by the Irish government, is low” and it was felt that that threats from natural disasters e.g. the Icelandic volcano, the flu pandemic and the Japanese Tsunami were more likely to be on organizational risk radars than terrorism.

Have large organizations improved their business processes over the past 5 years? If yes, has this improved their resilience?

Responses to this question focused on the fact that improvements in business processes such as Enterprise Risk Management (ERM), Enterprise Resource Planning (ERP), and Six Sigma have generally led to improved resilience. “Those who have implemented ERM will, as part of the process, look at risk mitigation firstly and then at continuity and contingency and so improve their resilience levels as a result”.

A word of warning was raised by respondents who said that “just-in-time (JIT) and lean business processes had also introduced more dependencies on others as inventory levels were often lower and as costs reduced, dependencies increased”. It was mentioned that one of the issues with ERP systems and processes was that “organizations now have reliance on one system as opposed to separate systems” as was the case in the past. Another point to note from responses was that the main driver for improved business processes was more likely a “financial/costs one” and not a “BCM/resilience one” and that there was a “conflict between financial pressures and BCM when it comes to keeping lean inventories”.

Have large organizations increased their investment in BCM over the past 5 years? If yes, has this improved resilience?

A mixed response was received from the respondents. Some responses said that over the last 5 years, certainly up until the economic downturn, “investments in BCM had increased in large organizations”. One respondent said that they did “not believe an increase occurred” with another saying they thought that “BCM investments would have remained static”. A provider of BCM facilities noted that “over the last 2 years many organizations have downsized their outsourced BCM capabilities”. The mixed response was very much dependent on what part of the industry respondents came from. For example providers of BCM facilities replied negatively while BCM consultants replied positively. Other comments of note were that “in general hot site and telecommunication costs have fallen over that period of time so organizations are now getting more services for the same level of investment” and also, from a consulting viewpoint, “more investments were being made into building resilient organizations”. It was mentioned that BCM is “a long process which is on-going” so as “organizations mature, investment will continue”. A further response noted that “improvements in resilience were not necessarily due to BCM but because of a greater appreciation of operational continuity issues”. A final response noted that “in some large organizations once the initial BC plan was completed the feeling was that there was no need for any more expense on it and that the budget was now invested in training and familiarisation of the BCM process with the ensuing increase in resilience capabilities”.

Do you think central government has taken a keener interest in the BCM capabilities of organizations over the past 5 years?

Responses to this question ranged from a definite “No” to a discussion of the fact that central government had improved their own internal BCM capabilities without taking an interest in the BCM capabilities of the wider business community. Notable responses were that at “at cabinet level they are probably not aware of what BCM stands for and at best gave it lip service”. It was mentioned that often “government give considerable consideration to IT recovery but often do not have people covered in their internal BCM processes”. A number of responses mentioned that the governments of the UK, Australia and New Zealand were more proactive in this regard with the UK, as an example, having national and community risk registers. It was felt that the Irish government had responded well to the Foot and Mouth incident and had also established the National Emergency Co-ordination Centre (NECC) which was useful but this was not focused on the BCM capabilities of organizations.

Have regulators taken a keener interest in the BCM capabilities of organizations over the past 5 years?

The impact on organizations of corporate governance and regulation is well noted in the literature as a BCM driver for change by Elliott, Swartz and Herbane (2010), O'Hehir (2007), Dye and Langsett (2008). In general the responses to this question were not flattering when viewed from an Irish regulatory perspective. In the area of telecommunications and food however the Irish regulators were noted as being active in the BCM area regarding food recall, traceability, telecommunications, power and link testing. Irish organizations subject to external regulations such as Sarbanes-Oxley (this legislation came into force in the USA in 2002 and introduced major changes to the regulation of financial practice and corporate governance), operating on a global basis and those in the financial and pharmaceutical sectors were more likely to have regulators taking an active interest in their BCM processes but from an Irish regulator perspective this was not the case. Some felt that the Irish regulators will "follow the lead of the USA and UK regulators eventually" but currently a lot of regulatory requirements represented a "tick in a box exercise in Ireland".

From what sources do you think organizations get their information on BCM?

Amongst the sources mentioned were: websites, including Continuity Central; professional bodies such as the Business Continuity Institute and the Emergency Planning Society; the British Standard 25999; good practice guidelines; BCM providers such as IBM and HP; seminars; insurers; peers (informal networks operate effectively in Ireland); and internal IT departments.

One interviewee thought "the source used depends on who is looking for BCM information". Key influencers in large organizations are more likely to read an article on BCM in the "Financial Times" rather than actively go looking for information elsewhere.

As an aside to this question it was noted that the membership of professional bodies such as BCI had “at best remained static over the past number of years in Ireland whilst growing internationally”. One respondent said they had also noticed that “a lot of BCM roles had been combined with other organizational roles rather than as a full standalone function”.

Do you think government agencies are used as a source of BCM information?

An overwhelmingly negative answer was received to this question. Respondents said that they did not know where responsibility lay for BCM within government in Ireland. In the UK, Canada, Australia and New Zealand the governments produced good guidelines. One response said that those looking for government guidelines were “more likely to use the UK as a starting point rather than to look for any in Ireland”. It was mentioned that the UK was more proactive in terms of trying to build a resilient society.

Within organizations, who do you think is usually:

a) responsible for Business Continuity Management?

b) involved in creating the Business Continuity Plan?

c) the owner of the plan and responsible for implemented?

Respondents said that responsibility for BCM normally resided with: the finance department; the IT/Chief Technical Officer (CTO); the operations department or operations director (in the case of the manufacturing sector); facilities managers; human resources; risk departments; or the company secretary. Respondents felt it was not good for BCM responsibility to lie within the finance department (from a BCM investment perspective) or within IT (as they have too many vested interests in BCM). They also felt it was poor practice, to run BCM as a “special project given to someone who is near retirement”. Respondents felt it was good practice to include BCM within: the corporate risk department (if a strong risk function existed); facilities or operations departments, depending on the sector in which they operate (in the manufacturing, food and pharmaceutical sectors).

Looking at who is involved in creating the BC plan, respondents said responsibility lay with:

- the IT department;
- with a specialist BCM coordinator, if they have that specific role;
- finance, who often delegate to IT or facilities,
- 3rd parties;
- operations or risk departments.

It was felt that, ”ideally each departmental manager should retain ownership and responsibility” and this should be “part of the individual key performance indicators for the manager to ensure it gets the required focus”.

The interviewees noted that plan ownership and responsibility for implementation was mainly at departmental/business unit or middle management level. These people would also be responsible for “exercising, reviewing and distributing the BC plan”. This is an noteworthy finding as references to the importance of senior management participation and backing are to be found in the literature as noted by Barnes (2001), Elliott, Swartz and Herbane (2010), Gallagher (2003), Koch (2004) and Seow (2009). Where IT had sole responsible for BCM then it was left with IT to implement it also. It was also stated that “nominally it was a senior manager who wrote the introduction to the BC plan but the actual owner was more at middle management level”.

Has BS25999 had a wide/significant impact on BCM in large organizations?

Those who provide BCM consultancy to organizations responded positively to this question stating that BS25999 had impacted on both large and small organizations as it gave them a standard to work to. The impact was particularly noted in the financial sector as it is now a recognised standard which has brought a focus onto BCM. In Ireland however “only one organization has currently been certified to the BS25999 standard”.

Other respondents however were less fulsome about the impact of BS25999 on BCM in Ireland saying that the main effect was that “vendors were saying they were creating BC plans to The Standard" or that "organizations were using the BCM lifecycle as a guide but not digging any deeper into The Standard". Other comments to note were that while consulting companies were using The Standard "most organizations dipped in and out of it to get guidelines and ideas" but it was doubtful if many would go for full certification unless "they were already ISO certified, in which case implementation of BS25999 was seen as easier". Other respondents gave a flat "None" to the level of impact made by BS25999 and said that "unless they were taking BCM seriously The Standard would not be known about".

To whom are organizations most likely to communicate their BC capabilities?

As outlined in the literature, The Standard, Barnes (2001), Elliott, Swartz and Herbane (2010) and Gallagher (2003) note that communicating the importance of the BCM programme to the whole organization and appropriate stakeholders is vital in order to keep it in focus.

Auditors, both internal and external, were identified as one of the groups who look at organizational BCM. Regulators and insurance companies sometimes required evidence of BCM capabilities depending on the sector in which the organization operated but this was often no more than a 'tick in the box' exercise. Respondents felt that organizations involved in a supply chain were "more likely to communicate their BC capabilities to their customers and key clients". Employees, shareholders, investors and internal stakeholders were only communicated with from a BCM perspective in organizations that had a mature BCM process in place. It was mentioned that "some large multinationals often declare their BCM capabilities upfront" but that this was mainly a media exercise.

Are more organizations insisting on their outsource suppliers having Business Continuity Plans now than in the past? If yes, how do you think these are verified?

As alluded to by Gallagher (2003), outsourcing of non-core functions and services presents BCM with a particular set of problems in that control for the outsourced function or service now resides with a third party. A firm "Yes" answer was received from all regarding this question. Until the year 2000, relating to Y2K projects, "everyone asked everyone else for their BC plans" but this requirement had lapsed. More recently organizations, due to their reliance on 3rd parties, had started to ask for evidence of BC plans. One of the main drivers was lean production processes where large inventories were not being held any longer and so manufacturing organizations were more reliant on suppliers. The requirement was also sectoral based particularly in the financial, pharmaceutical sectors but no evidence of this requirement was mentioned in the retail sector.

A mixed response was received when asking how organizations verify the fact that outsource suppliers have BC plans in place. Some organizations, who are more mature from a BCM perspective, will conduct combined testing and BCM exercises with suppliers, other organizations with less mature processes will "just want to see that a physical plan exists" whilst others will just undertake a "tick in the box" exercise with no actual testing taking place. It was mentioned that "depending on how much negotiating power the organization had over its outsourcers then its requirements for verification may be different" with the most powerful having higher requirement levels.

Do you think most large organizations have their own generators so that power outages will not materially affect their business?

Generally responses to this question were positive with some caveats. "Most large organizations that control their buildings and campus will have generators" but others who rent/share locations may need landlord or planning approval which may make it impossible to install a generator. Various concerns were voiced as to whether organizations that had generators actually tested them or were sure that the generators could support the actual power requirements needed when called upon. Some respondents commented that the requirement for generators "depends on where in the world you are". In India for instance power outages are expected so generators are used extensively whereas in Scandinavian countries the usage of generators is lower because power supply is viewed as reliable. Many organizations are happy to "just list a generator supplier in their BC plans" without actually installing one and it is only when a power issue is encountered that generator provision is actively looked at.

Do large organizations feel the power supply to their organization is reliable?

This question was answered positively; respondents believe that the power supply is reliable to large organizations. In the past large organizations may have felt that the power supply was not reliable but this "perception had lowered over the last number of years". However, a lingering concern was that of "industrial action taking place in power providers due to the limited number of supplier alternatives in Ireland".

Are some large organizations willing to accept the risks associated with power outages rather than invest in a backup power supply?

The majority of respondents said that many organizations are "willing to accept the risks associated with power outages" rather than invest in a backup power supply. It was noted that when an organization has a power related incident "only then will their attitude change" and while they may accept one power outage when "a second occurs they then have to do something serious about addressing the issue". It was also noted that some BCM outsource providers do not cover organizational incidents related to power outages so BCM support contracts may not be able to be activated for power issues.

Is BCM still focused on IT and Communications, as was the case in the past?

Most responses said that BCM had "moved on from purely being an IT and communications issue" as in the past. IT and communications were being treated more like any other service that organizations use to deliver their business. While they are core business services BCM has moved on. Some responses recognised that the view that "BCM was no longer focused on IT and communications" was sector dependent. In the pharmaceutical, service provider and manufacturing sectors where ‘just in time’ delivery, rapid response and low inventories were important, IT and communications may be more important than in other industries and so still has a focus on it for BCM purposes. Two of the respondents still felt that there remained a BCM focus on IT and communications as in the past in many organizations.

How frequently do you think organizations exercise their BC plans?

As noted in the literature by Gallagher (2003), Alexander (2005) and Bradbury (2008), it is important that the BC plans are subject to regular review, exercising and updating and that all areas of the organization are covered including the plans, the process, the people, and the infrastructure. Respondents in the main felt that organizations exercised their BC plans “at least annually” and “sometimes twice a year”. If organizations had a full hot site service, then “exercising a couple of times a year would be generally undertaken”. The depth of the exercises undertaken was questioned. Organizations are aware of the risks associated with conducting full blown exercises so these were conducted rarely and then only by large organizations who had a mature BCM program in place. It was felt that most tests were conducted at a departmental level rather than at a full organizational level. One respondent suggested that “because a lot of large organizations had a full hot site capability they were in fact testing on a 24*7*365 basis”.

Finally, what do you feel could be done to increase the uptake in BCM in large Irish organizations?

In order to increase the uptake of BCM in large organizations it was felt that central government and the regulators would need to be the key drivers of any improvement in the situation by moving to a resilient community approach, as is the case in the UK. One response mentioned the fact that from their perspective there seems to be “more happening with BCM at least internally in government departments” (for example, the Irish Revenue Commissioners recently received BS25999 certification) and that this should ultimately drive out into private organizations. Another interviewee felt that there has to be a “carrot and stick approach" taken by government regarding the uptake of BCM in large Irish organizations. It was also mentioned that Corporate Governance had a part to play. Another response suggested that "there should be tiered levels of BCM certification available as many organizations don't need or can't afford to have full BCM certification". This certification "could be driven through local interest groups, local authorities or the likes of the Institute of Directors, IBEC, BCI or the EPS". If the organization is involved in a supply chain then they are more likely to be effected by BCM issues and initiatives undertaken elsewhere in the chain. It was mentioned that a credible Irish standard should be established and that many large organizations were using global standards.

5.3 Conclusion

Responses from the interviews proved to be in-line with the main results from the survey. As the interviews were conducted with experts working in the area of BCM in Ireland and the interview question themes were derived from the survey, the results expand on the survey findings and add depth to the research as a whole. The results of the interviews will be included in Chapter 6 where conclusions and recommendations are outlined.

CHAPTER SIX

CONCLUSIONS AND RECOMMENDATIONS

6.1 Conclusions

6.1.1 Responsibility for BCM

The level of senior management involvement in leading and championing BCM is an issue of historical and on-going importance to those researching and studying continuity and resilience management. While there has been an improvement between the 2004 and 2009 surveys, generally responsibility for BCM does not rest at the top of respondent organizations but has been delegated to lower level management or to specialist roles/functions. Senior management should take responsibility for BCM strategy and in overseeing the development of robust, fully-rehearsed and well-communicated plans. It is vital that organizations ensure resilience in all mission critical elements of their business, this involves all directors, managers and employees being aware of their duties in the event of a disruption.

6.1.2 BCM Influenced by Sector and Regulation

The sector in which an organization operates has an impact on the significance attached to BCM. Financial, pharmaceutical and multinational organizations appear to take BCM more seriously than unregulated, indigenous Irish organizations. This may be due to the former as identified by Oldfield (2008b) as having developed supportive partnerships with critical stakeholders in the wider supply chain, sector and community

BCM was seen as being on the priority list for the organizations studied but it keeps getting moved down the list as competing priorities took precedence. Where regulation forces organizations to implement effective BCM it remained a high, strategic priority.

6.1.3 Threats to Continuity

This research identified that computer viruses/bugs and other IT related issues including communications link failure and system issues were considered the most likely cause of business disruption. The loss of IT capacity and telecoms were considered highly visible disruptions as they are core services for nearly all large organizations today. Irish organizations are also vulnerable in this area due to the fact that there are a limited number of telecoms suppliers operating in the Irish market.

Outside of IT, utility supply issues, leaks/water damage, supply chain problems were mentioned as issues of concern. It is interesting to note that a full blown building incident was rated as a low threat as the likelihood of occurrence was viewed as unlikely or “rare”. As noted by Sheffi (2007), the vulnerability of an organization to a disruptive event is made up of a combination of the likelihood of the disruption and its potential severity.

The threat posed by terrorist activity has decreased between the surveys. This drop may be particular to Ireland which has not suffered significant levels of terrorist activity over the past five years. The Northern Ireland Peace Process was highlighted as a major contributory factor to decreasing this threat to business continuity. It was also felt that the media had a role to play in this area as there were fewer headline terrorist incidents, such as 9/11, which contributed to terrorist threat perception levels being lower.

As organizations become leaner and downsize, primarily due to the current economic climate, the threat of loss of skills and people will continue to grow. Redundancies are a major cause of loss of people and skills as it is usually the older more experienced staff who are targeted in these initiatives. As noted by Perman (2009) organizations can experience large financial losses when they are unprepared for a key employee's departure. This can lead to further outsourcing of core skills if they cannot be sourced in-house. This may pose an additional threat as outsourcing will require better BCM ties with outsourcing partners to ensure that the outsourced activities can continue to function in the event of a business disruption.

6.1.4 Drivers of BCM.

Corporate governance was identified as the main driver for respondent organizations changing their approach to BCM. As noted by O'Hehir (2007), corporate governance is in place to balance and manage risk and implement internal control procedures on entrepreneurial energy. Large Irish organizations subject to external regulations such as Sarbanes-Oxley, operating on a global basis, and those in the financial and pharmaceutical sectors were more likely to have regulators taking an active interest in their BCM processes but from an Irish regulator perspective this was not the case. As noted by Elliott, Swartz and Herbane (2010), controls that come from outside the organization are usually imposed as the authority implementing them will probably have statutory powers to enforce compliance. It is expected that the Irish regulators will follow the lead of the USA and UK regulators eventually but currently a lot of regulatory requirements represent no more than a 'tick in a box' exercise in Ireland. The low level of government being seen as a driver for BCM is noteworthy in an Irish context. The fact that most of the drivers are external to the organization and that no internal drivers were identified other than internal audit, best practice and technology refreshes is also of note. It appears that only if organizations are forced to do so by external drivers will they address the issue of BCM.

6.1.5 Monitoring, Verifying and Communicating the BCM Capability

Auditors both internal and external are, as they were in 2004, the main group asking for evidence of BCM activity and competence. Regulators and insurance companies sometimes required evidence of BCM capability depending on the sector in which the organization operated but it was felt that this is often no more than a "tick in the box" exercise.

Those organizations who are involved in a supply chain were seen to communicate their BCM capabilities more to their stakeholders. One of the main reasons why evidence of BCM is required today is due to lean production processes where large inventories were not being held any longer and so manufacturing organizations were more reliant on suppliers. The requirement is also sectoral based, being particularly prevalent in the financial and pharmaceutical sectors.

There has been growth in organizations outsourcing non-core functions to 3rd party providers since the survey of 2004. A large number of organizations still rely on statements from their outsourcer in order to verify their BC plans.

The main groups to whom an organizations BC capabilities are communicated are Senior Management, then the Board followed by employees. These are all internal groups with external groups not communicated to in a similar fashion. The probable reasons for this trend are that BCM is still seen as a mainly internal process and external groups only get a view of these internal capabilities when they ask for them e.g. regulators, auditors, customers, suppliers etc. Very often external communication takes the form of a 'tick in a box' exercise and no actual physical evidence of a BCM process has to be provided. Employees, shareholders, investors and internal stakeholders are only communicated to from a BCM perspective in organizations that have mature BCM processes/programs in place.

6.1.6 The Impact of BS25999

The research shows that BS25999 has not had a great impact in large Irish organizations. Its impact was noted in the financial sector where it is now a recognised standard which has brought BCM into focus. In Ireland, however, only a small number of organizations have been certified to the BS25999 standard. Organizations are using the BCM lifecycle as a guide but are not 'digging any deeper' into The Standard. While consulting companies were using The Standard, most organizations dipped in and out of it to get guidelines and ideas. The low uptake in the use of BS25999 could, as identified during the interviews, be due to its complicated nature and the costs associated with implementing such a program.

6.1.7 Moving beyond IT

While progress has been made, the research identifies that BCM is still viewed as an IT problem with an IT focus in some organizations. Clearly IT is important from a continuity perspective but all mission critical activities need to be protected. It was in the pharmaceutical, service provider and manufacturing sectors, where 'just in time' delivery, rapid response and low inventories were important, that BCM was more likely to have moved beyond an IT-centred approach to BCM – without losing sight of the need to protect critical IT and communication systems. From the literature it is evident that the business and internal cultures of an organization have an important part to play in the way BCM is approached.

6.1.8 Ensuring Plans are Fit for Purpose

According to Alexander (2005) plans should be tested and updated periodically on a repetitive cycle. The research revealed that the majority of organizations (64%) exercised their BC plans at least annually and sometimes twice a year (28%), particularly if organizations had a full hot site service. The scope and depth of the exercises undertaken is still in question. Some respondents highlighted the risks associated with conducting full blown exercises. Comprehensive, organization-wide exercises were conducted rarely and then only by large organizations which had a mature BCM program in place. Most tests are conducted at a departmental level rather than at a full organizational level.

6.1.9 Investing in BCM

Budgets for BCM over the 5 years up to 2009 largely remained static. An interesting finding, given the current economic climate, was that 8% of respondents said that their BCM budgets would increase substantially and 23% reported that their BCM budgets would increase marginally in 2009. Only 4% said their BCM budget would decrease. In general hot site costs have come down during the five year period, as have telecommunications costs, so organizations are now getting more services for the same level of investment.

6.1.10 Maintaining a Power Supply

The research revealed that where the organizations controlled their buildings they normally have generators on site. However, where buildings are in rented/shared locations they may need landlord or planning approval which may make it impractical to install a generator. During the interviews concerns were raised as to whether organizations that had generators actually tested them or were sure that they could support the actual power requirements needed when called upon. It appeared that many organizations simply list a generator supplier in their BC plans without actually installing one – thus adopting a somewhat reactive approach to power management.

In the past large organizations felt that the power supply was rather unreliable but this perception had changed for the better between 2004 and 2009. However, one concern which remained was that of industrial action taking place in power providers due to the limited number of supplier alternatives available in Ireland.

6.1.11 Summary of Findings

In summary, the results of this study show that responsibility for BCM is firmly placed in the realm of senior and middle management with a low level of directorial or board-level involvement; computer viruses/bugs are viewed as the greatest threat to Business Continuity; loss of telecommunications is the most often experienced disruption; external rather than internal pressures drive most BCM activity; 89% of s have a regularly exercised BCP; and BS 25999 has not as yet had a wide impact in Irish organizations. Based on these findings a number of recommendations will be proposed, the aim of which will be the enhancement of BCM in large organizations in Ireland.

6.2 Recommendations

6.2.1 Protecting Technology

The threat of computer viruses to organizations can be circumvented by using adequate, up-to-date fire-walling and anti-virus software to ensure that computer viruses/bugs are blocked before they get into an organization's network. Internet and email access can be controlled via internet and email proxies to stop users downloading malicious software and end point security options are also available to cover the use of USB keys, CDs etc. These technologies should be adopted by organizations to ensure they are adequately protected.

The stability of the external telecommunications infrastructure needs to be addressed by 3rd party providers from an organizational view point. The main option available to organizations to avoid telecommunications outages is to install diverse vendor connections to try to ensure that if one vendor has an outage then the other will continue to function. This diversity comes at a financial cost however and may not always be physically possible due to the inability to source diverse vendors in certain locations.

While the use of technology continues to grow in organizations it must be noted that issues such as power failures (which rated highest in the 'serious category') still have an impact on organizations. By using generators and UPS the impact of power failures on organizations can be lessened.

6.2.2 Building Resilience Across the Organization

An organization wide resilience approach should be adopted by organizations to ensure that BCM is included from the start in any new business processes that are implemented. It is essential for the wider supply chain that appropriate BCM measures are put in place in organizations.

It is recommended that organizations rather than having separate processes for BCM, Crisis, Risk and Security Management need a more unified approach. The option of having an all-encompassing OR approach would provide a more connected framework and therefore ensure a better uptake across organizations and would also ensure that organizational BC plans were better integrated with the emergency services plans and processes. It is essential therefore that good programme management processes are put in place in order to have a successful and effective BCM programme.

6.2.3 Maintaining Skills/Personnel

In order to ensure that the organization has the relevant people and skills required to continue to function, it is recommended that organizations should implement cross training and succession planning programs and should also look at the option of buying in skills cover from 3rd parties in order to provide cover for skill or personal shortages should they arise.

6.2.4 Business Process Reengineering (BPR)

Business processes reengineering such as Enterprise Risk Management (ERM), Enterprise Resource Planning (ERP) and Six Sigma have generally led to improved resilience due to the fact that as part of the process organizations must look at risk mitigation firstly and then at continuity and contingency and so improve their resilience levels as a result.

The main driver for improved business processes is often a financial/costs reduction one and not a BCM/resilience one and there are often conflicts between financial pressures and BCM when it comes to keeping lean inventories. It should be borne in mind that when adopting BPR initiatives organizations need to ensure that BCM capabilities are maintained at adequate levels. Having good programme management in place in the organization will aid in successful and effective BCM.

6.2.5 Building Community Resilience

Communication of organizational business continuity capabilities needs to be more externally focused to ensure that disruptions do not impact the wider economy and also the public as a whole. This process should be driven by government by adopting a community resilience approach similar to that used in the UK.

6.2.6 A Role for Government

Irish central government needs to take a more active role in raising awareness of BCM within the economy in order to provide a more coordinated and controlled response in the event of a major disruption and to ensure society as a whole is more resilient. It is unclear where the responsibility for BCM lies within government in Ireland.

It is recommended that in order to increase the uptake and awareness of BCM, central government and the regulators should act as the key drivers in any improvement in the situation by moving to a resilient community approach as is the case in the UK. A government led initiative to encourage closer organizational integration with emergency services is also desirable.

A specific government department should be given overall responsibility for any initiatives in this area.

6.2.7 Increasing the Impact of BS25999

In order to increase the take up and impact of the BS25999 standard it is recommended that tiered levels of BCM certification should be made available. Many organizations don't need or cannot afford to have full BCM certification based on BS25999. Certification could be driven through local interest groups, local authorities or bodies such as the Institute of Directors, IBEC, BCI or EPS. It is further recommended that organizations use BS25999 in order to benchmarking their current BCM programme against in order to identify any gaps that exist.

6.2.8 Maintaining Resilience During the Recession

BCM should not be viewed as a luxury and something that is the first area to be cut in times of recession. Organizations need to ensure their BCM capabilities are not degraded as a result of the current economic conditions being experienced but are kept at the appropriate level to ensure business survival.

6.2.9 Senior Management Input

The role of senior management is key to ensuring the success of BCM within organizations. They should play their part when it comes to ensuring that the BCM programme is robust, fit for purpose and well-communicated to all organizational employees and stakeholders. All of the organizations employee should have some level of BCM responsibility built into their KPI's to ensure that it gets a continued focus.

6.2.10 HR Involvement

Too often the needs of employees are not addressed in BCM programmes. It is therefore crucial that the HR function helps to ensure that the BC plans address employee needs as well as those of the business in times of crisis.

6.2.11 Exercising BCM

It is recommended that organizations which have adopted BCM should implement a robust, frequent and all-encompassing programme of BCM exercises and tests to ensure that the BCM programme remains up to date and is embedded into the organizational culture.

6.2.12 BCM and the Supply Chain

In order to ensure enhanced supply chains further closer links via the BCM programme need to be established with essential suppliers and outsourced providers in particular. This recommendation will ensure that all participants both up and down the supply chain will have confidence in each other's abilities to survive crises.

6.3 Research Review and Recommendations for Further Research

This research provides an update on the position of BCM in large Irish organizations from the research conducted in 2004. Similar issues and challenges exist for the implementation of BCM in both surveys. The global recession, the ever expanding use of supply chains and a wide range of new technology threats have made the implementation of BCM programmes even more vital than they were in the past in order to ensure the survival of organizations who suffer crisis events.

The research tools used were deemed appropriate for the task in order to allow for a comparison to take place between the two bodies of research but further research is merited into the area of BCM.

The following suggestions may be useful in aiding further research studies relating to BCM in Irish organizations:

- Perform a more in depth study into the respondent organizations to determine the effectiveness of their BCM strategies.
- Examine the extent of the application of BCM within Irish SME's to get a better understanding as to where the practice stands in the wider business context from a domestic point of view.
- Conduct more comprehensive interviews with BCM practitioners across the country in order to get a deeper insight into how BCM is implemented and also to gather more views from different practitioners within the BCM space.
- Run a number of in depth case studies across industry sectors with large organizations to see the specific issues they face when implementing BCM programmes.
- If possible get a response from government on their stance with regards to BCM and the wider community and investigate how government approaches BCM internally.
- Perform further research into the impact of organization culture and communications theory on BCM.

6.4 Significance of the Research

This research and its predecessor are significant in that in 2004 it was the first study of its kind to have been conducted in Ireland. The current research therefore provides an update on the 2004 survey and therefore gives us a view of the evolution of BCM in large Irish enterprises over a 5 year period. The research also adds further to the understanding of how the concept of BCM is applied within large Irish enterprises and endeavours to open up the topic to encourage further research and debate within the wider BCM industry in Ireland.

At the outset of the study it was agreed that the purpose of the thesis was to show the evolution of BCM in large Irish organizations between 2004 and 2009. This was done through interviews, literature review and the survey. However it must be noted that a more in depth investigation into the BCM practices of the respondent organizations is the next logical step.

As Horne III (1997) concludes:

> "The blisteringly fast rise of the Internet is certainly proof of the speed with which people can adapt to a world full of varied, far-distant connections to create their own communities with resilient properties. In these new living systems, the course of change is not always predictable, and small events can exert far-reaching influence. Thus, the coming age of organizational resilience and all it embodies is upon us." (Horne III 1997, p. 28)

REFERENCES

Adkins, L. Thornton J. and Blake, K. (2009). A content analysis investigating relationships between communication and business continuity planning, *Journal of Business Communication*, 46(3), pp 362-403.

Alesi, P. (2008). Building enterprise-wide resilience by integrating business continuity capability into day-to-day business culture and technology, *Journal of Business Continuity & Emergency Planning,* 2(3), pp. 214–222.

Alexander, D. (2005). Towards the development of a standard in emergency planning, *Disaster Prevention and Management*, 14(2), pp. 158-175.

Aronson, E. 1999. *The Social Animal*, Worth publishers, United States of America: W.H. Freeman and Company.

Arif, M. 2007. Recovery Strategies, *Computer Weekly*; 11/13/2007, pp. 34-36. Available from: http://web.ebscohost.com/ehost/detail?sid=15b0c5f2-0875-4746-991d-40428145ab6e%40sessionmgr104&vid=1&hid=111&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=27820799. [Accessed November 2009].

Armit, T. 2007. BCP Plan Testing *IN:* Hiles, A. (ed) *The Handbook Of Business Continuity Management*, Second Edition, England: John Wiley & Sons Ltd, pp.323-338.

Barnes, J. 2001. *A Guide to Business Continuity Planning*, England: John Wiley & Sons Ltd.

Barnes, P. 2007. Business Impact Analysis *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp.145-160.

Basel Committee on Banking Supervision 2006: *High-level principles for business continuity*. Basel. Switzerland. Bank for International Settlements. [Online]. Available from: http://www.bis.org/publ/joint17.pdf [Accessed Dec 2010].

BCI, *Certification Standards*. The Business Continuity Institute. [Online]. Available from: http://www.thebci.org/certificationstandards.htm. [Accessed Jan 2011].

BCI 2002, *Business Continuity Management- Good Practice Guidelines*. The Business Continuity Institute. [Online]. Available from: http://www.security.auckland.ac.nz/images/BCIGPGIntroduction.pdf. [Accessed Jan 2011].

BCI 2011, *Dictionary of Business Continuity Management Terms*. The Business Continuity Institute. [Online]. Available from: http://www.thebci.org/glossary.pdf. [Accessed January 2011].
www.bci.org,. Certification Standards, Available from: http://www.thebci.org/certificationstandards.htm. [Accessed November 2009]

Beatty, C. 2007. Emergency response and operations *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, p. 269.

Bell, J. 2005: *Doing your research project,* Maidenhead: Open University Press.

Benbasat, I., Goldstein, D.K. and Mead, M. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly* (11:3) 1987, pp. 369-386.

Birk, S. 2009. Creating of a culture of safety: Why CEOs hold the key to improved outcomes. *Healthcare Executive*, Mar/Apr2009, Vol. 24 (2), pp. 14-22.

Boin, A. 2009. The New World of Crises and Crisis Management: Implications for Policymaking and Research, *Review of Policy Research*; Jul 2009, Vol. 26 (4), pp. 367-377.

Bradbury, C. 2008. Disaster! Creating and testing an effective recovery plan. *British Journal of Administrative Management*, April 2008 (62), pp.14-16.

Brazeau, P. 2008. Holistic Protection, *Canadian Underwriter*, Vol. 75 (3), pp. 26-28.

British Continuity Institute, 2002. *Good Practice Guidelines*, London: Business Continuity Institute.

Brouggy, P. 2009. Resilient maturity model analysis, *BCI Continuity Forum*. Available from: http://www.thebci.org.au/images/documents/events/35___P%20Brouggy%20Resilience%20Present%20v2_10-09-09.pdf. [Accessed July 2010].

BSI 2006, BS 25999-1:2006. *Business continuity management – Part 1: Code of practice*, England: British Standard Institute, ISBN 0 580 49601 5.

Burke ,S. Wilson, K. Salas, E. 2005.The use of a team-based strategy for organizational transformation : guidance for moving toward a high reliability organization. *Theoretical Issues in Ergonomics Science*, November 2005. Vol. 6 (6), pp. 509-530.

Carson, D. Gilmore, A. Perry, C. Gronhaug, K. (2001).*Qualitative marketing research*. London: Sage Publications.

Castillo, C. 2004. Disaster Preparedness and Business Continuity Planning at Boeing: An Integrated Model. *Journal of Facilities Management*, 3(1), June 2004, pp. 8-26.

Chadwick, T. 2001. Setting the scene – e-BCM Issues. Continuity, *The Journal of the Business Continuity Institute*, Winter 2001, Vol 5(4), p 7.

Charters, I. 2007. Risk evaluation and control: practical guidelines for risk assessment *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 137 – 143.

Chen, Su-Shing. 2007. Digital Preservation: Organizational Commitment, Archival Stability, and Technological Continuity. *Journal of organizational computing and electronic commerce*, 17(3), pp. 205–215.

CIO.com: *Business Continuity and Disaster Recovery Planning Definition and Solutions* [Online], Available from: http://www.cio.com/article/40287/Business_Continuity_and_Disaster_Recovery_Planning_Definition_and_Solutions#1. [Accessed January 2011].

Civil Contingencies Act 2004. [Online], Available from: http://www.legislation.gov.uk/ukpga/2004/36/contents. [Accessed March 2010]

Coles, E. and Buckle, P. 2004. Developing Community Resilience as a foundation of effective Disaster Recovery, *Australian Journal of Emergency Management*, Vol19 (4), pp. 6 – 15.

Collicutt, J. 2008. Community resilience: The future of business continuity. *Journal of Business Continuity & Emergency Planning*, Vol. 3 (2), pp. 145–152.

Coutu, D. 2002. How Resilience Works. *Harvard Business Review*, May 2002, 80 (5), pp. 46-51.

Courtney, N. 2007. Developing business continuity strategies for the business or work areas *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, p. 161-172.

Creswell, J.W. 1994. *Research design: Qualitative and quantitative approaches*, Thousand Oaks, California: Sage.

Crichton, M. Ramsay, C. Kelly, T. 2009. Enhancing Organizational Resilience Through Emergency Planning: Learnings from Cross-Sectoral Lessons. *Journal of Contingencies and Crisis Management*, March 2009. 17(1), pp. 24 -37.

Cummings, J. 2003. Nurturing a culture of continuity. *Network World October*, 20(42), pp. 54 - 56.

Daft, R. 2001. *Organization Theory and Design*, 7th Edition, Ohio: South Western.

Denscombe M. 2007. *The Good Research Guide for small-scale social research projects*. 3rd edition. McGraw Hill.

Department of Environment Heritage and Local government 2006: *A Framework for Major Emergency Management*. Available from: http://www.dohc.ie/publications/pdf/major_emergency.pdf?direct=1. [Accessed January 2010].

De Vaus, D.A. (2002). "Surveys in Social Research",(5th ed), London, Routledge.

De Waal, A. 2006. Towards a comparative political ethnography of disaster prevention. *Journal of International Affairs*, Spring/Summer2006, Vol59 (2), pp.129-149.

De Witte, K. van Muijen, J. 1999. Organizational Culture, *European Journal of Work and Organizational Psychology*, Vol 8 (4), pp. 497-502.

Dye, K. Langsett, M. 2008. A roadmap to measure and achieve enterprise operational resiliency. *Journal of Business Continuity & Emergency Planning,* Vol. 3(1), pp. 38–46.

Dynes, R. Quarantelli, E. 1977. *Organizational communications and decision making in a crisis*, University of Delaware, Disaster Research Centre, Newark, DE I 19716, Report Series, 17. Available from: http://dspace.udel.edu:8080/dspace/bitstream/19716/1264/1/RS17.pdf. [Accessed January 2010].

Elliott, D. 2009. The Failure of Organizational Learning from Crisis – A Matter of Life and Death? *Journal of Contingencies and Crisis Management*, Vol 17(3), pp. 157-168.

Elliott, D. Johnson, N. 2010. A Study of Resilience and Business Continuity Practice 2010. *Business Continuity Project Final report,* University of Liverpool Management School, p. 47.

Elliott, D. Swartz, E. and Herbane, B., 2002. *Business Continuity Management – A crisis management approach*, London: Routledge.

Elliott, D. Swartz, E. and Herbane, B., 2010. *Business Continuity Management – A crisis management approach*, (2nd ed), London: Routledge.

Ellwood, A. 2009. Using the disaster crunch/release model in building organisational resilience. *Journal of Business Continuity & Emergency Planning*, Vol 3(3), pp. 241-247.

EU Council 2008, *European Critical Infrastructure*, *Factsheet 2008*, Justice and Home Affairs Council, Luxembourg, Available from:

http://www.eurunion.org/partner/euusterror/EUCritInfrastructFactsheet-6-5-08.pdf. [Accessed September 2009].

European Commission 2010, Available from: http://ec.europa.eu/environment/emas/emasawards/awards.htm. [Accessed February 2011].

Fink, S. 1986. *Crisis Management*, New York: AMACOM, American Management Association.

Fritzon, A. Ljungkvist, K. Boin, A. Rhinard, M. 2007. Protecting Europe's Critical Infrastructures: Problems and Prospects. *Journal of Contingencies and Crisis Management*, Vol 15(1), March 2007, pp. 30–41.

Gallagher, M. 2003. *Business Continuity Management - How to protect your company from danger*, FT Prentice Hall, London, England: Pearson Education Limited.

Gallagher, M. 2011. Business Continuity Management 'Do you measure up'. *Continuity Central*. Available from: http://www.continuitycentral.com/selfassessment.pdf. [Accessed January 2011].

Galliers, R.D. (1991) Choosing appropriate information systems research approaches: a revised taxonomy. In: *Information Systems Research: Contemporary Approaches and Emergent Traditions*, Nissen, H.-E., Klein, H.K. & Hirschheim, R. (eds), pp. 327–345. Elsevier Science Publishers, North Holland.

Ginn, R. 1992. *Continuity Planning – Preventing, Surviving and Recovering from Disaster*, Oxford, England: Elsevier Science Publishers Ltd.

Herbane, B. 2010. The evolution of business continuity management: A historical review of the practices and drivers. *Business History*, 52:6, pp. 978-1002.

Herbane, B. Elliot, D. and Swartz, E. 1997. Continuity and continua: Achieving excellence through business continuity planning. *Business Horizons*, (November-December), (1997): Vol 40(6), pp. 19-25.

Hiles, A. 2007a. An Introduction to business continuity planning *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. xix-xxvii.

Hiles, A. 2007b. Developing and implementing the written plan *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 279-314.

Hiles, A. 2007c. Awareness and training *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 315-322.

Horne, J. and Orr, J. 1998. Assessing behaviours that create resilient organizations. *Employment Relations Today*, 24(4), pp. 29–39.

Horne III, J. 1997. The coming age of organizational resilience. *Business Forum*, Spring/Fall97, Vol 22 (2/3/4), pp. 24-28.

Howe, J. 2007. Project initiation and management *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 122.

www.knowledgetransfer.net. *Business Continuity Management (ITILv3)*. Available from: http://www.knowledgetransfer.net/dictionary/ITIL/en/Business_Continuity_Management.htm. [Accessed Dec 2010].

Jackson, R. 2006. Business continuity: Preparation over Prevention. *Accountancy Ireland*, Dec 2006, Vol. 38(6), pp. 51-53.

Johnson, G. Scholes, K. 2002. *Exploring Corporate Strategy*, Sixth Edition, England: Pearson Education Limited.

Kaplan, B. & Duchon, D. (1988). "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study", *MIS Quarterly*, December, pp. 571-586.

Kello, J. 2009. How to assess your culture. *Industrial Safety & Hygiene News*, Jun 2009, Vol. 43(6), pp. 24-26.

Kelly, M. & McMullan, C. 2011, *Implementing Business Continuity Management – Sharing Good Practice from an Irish Context.* 1st International Conference on Safety and Crisis Management in the Construction, Tourism and SME Sectors (1st CoSaCM)

Khazanchi, D. and Munkvold, B. 2000. *Is information system a science?* An inquiry into the nature of the Information Systems discipline. SIGMIS Database, 31(3), pp.24-42.

Kjærgaard, A. 2009. Organizational Identity and Strategy. *International Studies of Management and Organization*, Vol. 39(1), pp. 50–69.

Koch, R. 2004. Best practices in business continuity. *Communications News*, Vol. 41(11), Nov 2004, p 24.

Kotnour, T. 2009. Putting Culture to Work in Our Organizations. *Engineering Management Journal,* June 2009,Vol. 21(2), p 1-2.

Lagadec, P. 2009. A New Cosmology of Risks and Crises: Time for a Radical Shift in Paradigm and Practice. *Review of Policy Research*, Jul 2009, Vol. 26(4), pp. 473-486.

LaPorte, Todd R. 1996. High Reliability Organizations: Unlikely, demanding, and at risk. *Journal of Contingencies and Crisis Management,* Vol. 4, p. 63.

LaPorte, T R. and Consolini, P. 1991. Working in Practice But Not in Theory: Theoretical Challenges of High-Reliability Organizations. *Journal of Public Administration Research and Theory*, Vol. 1, pp. 19–47.

Lengnick-Hall C. and Beck T. 2008. Resilience Capacity and Strategic Agility: Prerequisites for Thriving in a Dynamic Environment, The University of Texas at San Antonio, College of business. Available from: http://business.utsa.edu/wps/mgt/0059MGT-199-2009.pdf. [Accessed July 2010].

Lindstedt, D. 2007. Grounding the discipline of business continuity planning: What needs to be done to take it forward? *Journal of Business Continuity & Emergency Planning*, Vol. 2 (2), pp. 197–205.

Luthans, F. 2002. *Organizational Behaviour*, New York: McGraw-Hill.

Maxwell, J. 1996. *Qualitative research design: An interactive approach*, Thousand Oaks, CA: Sage.

Mitroff, I. 2001. *Managing Crises Before They Happen: What Every Executive and Manager Needs to Know About Crisis Management*, New York: Amaco.

Mitroff, I. Pauchant, T. Finny, M. and Pearson, C. 1989. Do (some) organizations cause their own crisis? Culture profiles of crisis-prone versus crisis-repaired organizations. *Organization & Environment,* 3(4), pp 269-83.

Mitchell, V (1996). “Assessing the reliability and validity of questionnaires: an empirical example”, *Journal of Applied Management Studies*, Vol 5:2, pp. 199-207.

Myers, K. 2006. *Business Continuity Strategies: Protecting Against Unplanned Disasters*, Hoboken, New Jersey: John Wiley & Sons, Inc.

National Organisational Resilience Framework workshop. 2007. “*The Outcomes: Business Continuity Management Information Exchange.”*. Available from: http://www.bcmie-australia.org/Download/Final%20Report.pdf.

[Accessed November 2009].

Nollau, B. 2009. Disaster Recovery and Business Continuity. *Journal of GXP Compliance,* Summer 2009, 13(3), pp. 51-59.

O'Hehir, M. 2007. What is a business continuity planning (BCP) strategy *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 27-45.

O'Leary, Z. (2004). *The Essential Guide to Doing Research*. London: Sage Publications.

Oldfield, R. 2008a. Organizational resilience. *Continuity Central*. Available from: http://www.continuitycentral.com/feature0618.html. [Accessed November 2009].

Oldfield, R. 2008b. So what is resilience and what benefits does it offer?. Available from: http://www.organisationalresilience.com.au/files/orgresilaug08.pdf. [Accessed November 2009].

Oriesek, D. Schwarz, J. 2008. *Business War gaming*, Burlington, USA: Ashgate Publishing Company.

Panko, R. 1987.Directions and issues in end user computing.*INFOR*, Vol. 25(3), pp.181-197. Available from: http://web.ebscohost.com/ehost/detail?vid=14&hid=5&sid=f593c135-32a0-4721-9c2b-9ae42b4d0311%40sessionmgr4&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=6284293. [Accessed October 2009].

Pas 56. 2003. *An Overview from automata, 2005*. Available from: http://www.automataservices.com/PAS%2056%20Overview1.doc. [Accessed October 2009].

Perman, G. 2009. Why Succession Management Matters. *CIO Insight*, Issue 103, pp. 34-36. Available from: http://web.ebscohost.com/ehost/detail?vid=16&hid=103&sid=3e294d01-2636-4d8f-8025456804bf6b5%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=38423726. [Accessed January 2010].

Preimesberger, C. 2009. Unfettered data growth challenges business continuity technology. *eWeek*, Vol 26(6), pp. 16-18. Available from: http://web.ebscohost.com/ehost/detail?vid=4&hid=108&sid=38e70d3f-627f-4625-832cafb2bbe916fc%40sessionmgr110&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=37334477#db=buh&AN=37334477. [Accessed November 2009].

Remenyi, D. Williams, B. Money, A. and Swartz, E. 1998. *Doing Research in Business and Management, An Introduction to Process and Method*, London: Sage.

Rhinard, M. 2009. European Cooperation on Future Crises: Toward a Public Good. *Review of Policy Research*; Vol. 26(4), pp. 439-455.

Riolli, L. and Savicki, V. 2003. Information system organizational resilience. *International Journal of Management Science*, Omega, 31, Elsevier Science Ltd, pp. 227-233.

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

Rossing von, R. 2007. BC Audit *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, p. 339.

Rugg G. & Petre M. 2007. *A gentle guide to research methods*. Open University Press.

Saunders, Lewis and Thornhill, 2007. *Research Methods for Business Students*, Harlow, Essex, England: Pearson Education Limited.

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

Sheffi, Y. 2007. *The Resilient Enterprise*, Cambridge, Massachusetts: The MIT Press.

Sheffi Y. and Rice Jr, J. 2005. Building the Resilient Enterprise, *MIT Sloan Management Review*, Fall 2005, Vol 42(1).

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), pp. 221-239.

Sikich, G. 2003. *Integrated business continuity: maintaining resilience in uncertain times*, Oklahoma, USA: PennWell.

Smith D. 2005. Business (not) as usual: crisis management ,service recovery and the vulnerability of organisations. *Journal of Services Marketing,* Vol 19(5), 2005, pp. 309–320.

Smith, M. and Sherwood, J. 1995. Business Continuity Planning, *Computers and Security*, 14(1), pp. 14-23.

Smith, M and Shields, P-A. 2007. Strategies for IT and communications *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, p. 205.

Somers, S. and Svara J. 2009. Assessing and Managing Environmental Risk: Connecting Local Government Management with Emergency Management. *Public Administration Review*, Mar/Apr2009, Vol. 69(2), pp.181-193.

Spigener, J. 2009. Can you recognize "exposure creep"? *Industrial Safety & Hygiene News*, Jun 2009, Vol. 43(6), pp. 44-46.

Stucke, C. Straub, D. and Sainsbury, R. 2008. Business Continuity Planning and the Protection of Informational Assets. *IN:* Straub, D. Goodman, S. Baskerville, R.(ed's). *Information Security Policies and Practices*, Armonk, NY: M.E. Sharpe, pp.152-172. Available from:
http://www.cis.gsu.edu/~dstraub/Present/2008/bcppaper.pdf.
[Accessed November 2010].

Sun Tzu. "*The Art of War*", 544-496 BC.

Swartz, E. Elliott, D. and Herbane, B. 1995. Out of sight, out of mind: the limitations of traditional information systems planning, *Facilities*, Vol 13(9/10), pp. 15–21. Available from:
http://www.ingentaconnect.com/content/mcb/069/1995/00000013/F0020009/art00003
. [Accessed October 2009].

Swiss Federal Banking Commission (SFBC). 2007. *Recommendations for Business Continuity Management (BCM)*. p. 4. Available from:
www.swissbanking.org/en/11107_e.pdf. [Accessed December 2010].

Taleb, N. 2007. *The Black Swan*, London, England: Penguin Books.

Turner, B. 1976. The organizational and inter-organizational development of disasters. *Administrative Science Quarterly*, 21, pp. 378-89.

Vaid, R. 2008. How are operational risk and business continuity coming together as a common risk management spectrum?. *Journal of Business Continuity & Emergency Planning*, Vol. 2(4), pp. 330–339.

Viner, P. 2007. Operational Risk Management *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 83-96.

Vizard, M. 2008. Why there's no business continuity. *Baseline*, Sep 2008, Issue 88, p 18. Available from:

http://web.ebscohost.com/ehost/detail?vid=6&hid=108&sid=38e70d3f-627f-4625-832cafb2bbe916fc%40sessionmgr110&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=34222133.
[Accessed January 2010].

Wack, P. 1985. Scenarios: uncharted waters ahead. *Harvard Business Review*, September-October 1985, pp. 73-89.

Whittet, L**.** 2008. Operational risk management and business continuity. *Continuity Central*, Available from: http://www.continuitycentral.com/feature0606.html. [Accessed January 2010].

World Economic Forum. 2008. *Global Risks 2008*. Available from: http://www.weforum.org/pdf/globalrisk/Risk08.pdf. [Accessed October 2009].

Youngblood, M. D. 2000. Winning cultures for the new economy. *Strategy & Leadership*, 28(6), pp. 4-10.

Zollo, M. Minoja, M. Casanova, L. Hockerts, K. Neergaard, P. Schneider, S. and Tencati, A. 2009.Towards an internal change management perspective of CSR: evidence from project RESPONSE on the sources of cognitive alignment between managers and their stakeholders, and their implications for social performance. *Corporate Governance*, Vol 9(4), pp. 355-372.

BIBLIOGRAPHY

Abercrombie, G. 2007. Who's Your Weak Link? *Harvard Business Review*, Vol. 85(12), pp.15-16. Available from: http://web.ebscohost.com/ehost/detail?vid=15&hid=103&sid=3e294d01-2636-4d8f-8025-1456804bf6b5%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=27439396

[Accessed November 2009].

Adkins, L. Thornton J. and Blake, K. (2009). A content analysis investigating relationships between communication and business continuity planning, *Journal of Business Communication*, 46(3), pp 362-403.

Aiken, C. and Keller, S. 2007. The CEO's role in leading transformation. *Management Quarterly*, Vol. 48(2), pp. 30-39. Available from: http://web.ebscohost.com/ehost/detail?vid=8&hid=108&sid=378db3e3-ded7-4c3e-b67b-dd7025a295e5%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=26243810. [Accessed December 2009].

Alesi, P. (2008). Building enterprise-wide resilience by integrating business continuity capability into day-to-day business culture and technology, *Journal of Business Continuity & Emergency Planning,* 2(3), pp. 214–222.

Alexander, D. (2005). Towards the development of a standard in emergency planning, *Disaster Prevention and Management*, 14(2), pp. 158-175.

Aronson, E. 1999. *The Social Animal*, Worth publishers, United States of America: W.H. Freeman and Company.

Arif, M. 2007. Recovery Strategies, *Computer Weekly*; 11/13/2007, pp. 34-36. Available from: http://web.ebscohost.com/ehost/detail?sid=15b0c5f2-0875-4746-991d-40428145ab6e%40sessionmgr104&vid=1&hid=111&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=27820799. [Accessed November 2009].

Armit, T. 2007. BCP Plan Testing *IN:* Hiles, A. (ed) *The Handbook Of Business Continuity Management*, Second Edition, England: John Wiley & Sons Ltd, pp.323-338.

Bajgoric, N. Moon, Y. 2009. Enhancing systems integration by incorporating business continuity drivers, *Industrial Management & Data Systems*, Volume 109(1), pp 74-97.

Barnes, J. 2001. *A Guide to Business Continuity Planning*, England: John Wiley & Sons Ltd.

Barnes, P. 2007. Business Impact Analysis *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp.145-160.

Basel Committee on Banking Supervision 2006: *High-level principles for business continuity*. Basel. Switzerland. Bank for International Settlements. [Online]. Available from: http://www.bis.org/publ/joint17.pdf [Accessed Dec 2010].

BCI, *Certification Standards*. The Business Continuity Institute. [Online]. Available from: http://www.thebci.org/certificationstandards.htm. [Accessed Jan 2011].

BCI 2002, *Business Continuity Management- Good Practice Guidelines*. The Business Continuity Institute. [Online]. Available from: http://www.security.auckland.ac.nz/images/BCIGPGIntroduction.pdf. [Accessed Jan 2011].

BCI 2011, *Dictionary of Business Continuity Management Terms*. The Business Continuity Institute. [Online]. Available from: http://www.thebci.org/glossary.pdf. [Accessed January 2011].
www.bci.org,. Certification Standards, Available from: http://www.thebci.org/certificationstandards.htm. [Accessed November 2009]

Beatty, C. 2007. Emergency response and operations *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, p. 269.

Bell, J. 2005: *Doing your research project,* Maidenhead: Open University Press.

Benbasat, I., Goldstein, D.K. and Mead, M. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly* (11:3) 1987, pp. 369-386.

Birk, S. 2009. Creating of a culture of safety: Why CEOs hold the key to improved outcomes. *Healthcare Executive*, Mar/Apr2009, Vol. 24 (2), pp. 14-22.

Boin, A. 2009. The New World of Crises and Crisis Management: Implications for Policymaking and Research, *Review of Policy Research*; Jul 2009, Vol. 26 (4), pp. 367-377.

Bradbury, C. 2008. Disaster! Creating and testing an effective recovery plan. *British Journal of Administrative Management*, April 2008 (62), pp.14-16.

Brazeau, P. 2008. Holistic Protection, *Canadian Underwriter*, Vol. 75 (3), pp. 26-28.

British Continuity Institute, 2002. *Good Practice Guidelines*, London: Business Continuity Institute.

Brouggy, P. 2009. Resilient maturity model analysis, *BCI Continuity Forum*. Available from: http://www.thebci.org.au/images/documents/events/35___P%20Brouggy%20Resilience%20Present%20v2_10-09-09.pdf. [Accessed July 2010].

BSI 2006, BS 25999-1:2006. *Business continuity management – Part 1: Code of practice*, England: British Standard Institute, ISBN 0 580 49601 5.

Business Continuity Institute and Continuity Forum, 2009. *Australia - New Zealand Business Continuity Benchmarking Survey 2009*, Available from: http://www.thebci.org.au/images/documents/news/19___BCI-CF%20BC%202009%20Survey%20-%20Summary%20v1.0.pdf. [Accessed November 2009].

Burke ,S. Wilson, K. Salas, E. 2005.The use of a team-based strategy for organizational transformation : guidance for moving toward a high reliability organization. *Theoretical Issues in Ergonomics Science*, November 2005. Vol. 6 (6), pp. 509-530.

Butler, B. 2005. Business Continuity Management: *A Positive Perspective on the Design of Resilient Organizations*. Katz Graduate School of Business University of Pittsburgh.

Carson, D. Gilmore, A. Perry, C. Gronhaug, K. (2001).*Qualitative marketing research*. London: Sage Publications.

Castillo, C. 2004. Disaster Preparedness and Business Continuity Planning at Boeing: An Integrated Model. *Journal of Facilities Management*, 3(1), June 2004, pp. 8-26.

Chadwick, T. 2001. Setting the scene – e-BCM Issues. Continuity, *The Journal of the Business Continuity Institute*, Winter 2001, Vol 5(4), p 7.

Charters, I. 2007. Risk evaluation and control: practical guidelines for risk assessment *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 137 – 143.

Chen, Su-Shing. 2007. Digital Preservation: Organizational Commitment, Archival Stability, and Technological Continuity. *Journal of organizational computing and electronic commerce*, 17(3), pp. 205–215.

CIO.com: *Business Continuity and Disaster Recovery Planning Definition and Solutions* [Online], Available from: http://www.cio.com/article/40287/Business_Continuity_and_Disaster_Recovery_Planning_Definition_and_Solutions#1. [Accessed January 2011].

Civil Contingencies Act 2004. [Online], Available from: http://www.legislation.gov.uk/ukpga/2004/36/contents. [Accessed March 2010]

Coles, E. and Buckle, P. 2004. Developing Community Resilience as a foundation of effective Disaster Recovery, *Australian Journal of Emergency Management*, Vol19 (4), pp. 6 – 15.

Coleman,L. 2006. Frequency of Man-Made Disasters in the 20th Century. *Journal of Contingencies and Crisis Management,* Vol 14(1), pp 3 – 11.

Collicutt, J. 2008. Community resilience: The future of business continuity. *Journal of Business Continuity & Emergency Planning*, Vol. 3 (2), pp. 145–152.

Cornelius, P. Van de Putte, A. and Romani, M. 2005. Three Decades of Scenario Planning in Shell. *California Management Review*, Vol. 48(1), pp. 92-109. Available from: http://web.ebscohost.com/ehost/detail?vid=11&hid=5&sid=58b56019-652a-4b27-966e-a0e54a4eff3f%40sessionmgr11&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=19077695. [Accessed September 2009].

Coullahan, R. Shepherd,C. 2008. Enhancing enterprise resilience in the commercial facilities sector, *Journal of Business Continuity & Emergency Planning,* Vol. 3(1), pp. 5–18.

Council on Competitiveness. 2008. *Enterprise Resilience*. Available from: http://www.compete.org/images/uploads/File/PDF%20Files/Prepare%20112008.pdf [Accessed December 2009].
Coutu, D. 2002. How Resilience Works. *Harvard Business Review*, May 2002, 80 (5), pp. 46-51.

Courtney, N. 2007. Developing business continuity strategies for the business or work areas *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, p. 161-172.

Creswell, J.W. 1994. *Research design: Qualitative and quantitative approaches*, Thousand Oaks, California: Sage.

Crichton, M. Ramsay, C. Kelly, T. 2009. Enhancing Organizational Resilience Through Emergency Planning: Learnings from Cross-Sectoral Lessons. *Journal of Contingencies and Crisis Management*, March 2009. 17(1), pp. 24 -37.

Cummings, J. 2003. Nurturing a culture of continuity. *Network World October*, 20(42), pp. 54 - 56.

David, A.2005.Towards the development of a standard in emergency planning. *Disaster Prevention and Management*, Vol. 14(2),pp. 158-175. Available from: http://first.emeraldinsight.com/articles/planning.htm. [Accessed February 2010].

Daft, R. 2001. *Organization Theory and Design*, 7th Edition, Ohio: South Western.

Davis, G. 2009. The Rise and Fall of Finance and the End of the Society of Organizations. *Academy of Management Perspectives*, Vol 23(3), pp.27-44. Available from: http://web.ebscohost.com/ehost/detail?vid=7&hid=108&sid=a179dc34-af77-431a-a2d0-b378ec56492b%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=43479262. [Accessed December 2009].

Denscombe M. 2007. *The Good Research Guide for small-scale social research projects*. 3rd edition. McGraw Hill.

Department of Environment Heritage and Local government 2006: *A Framework for Major Emergency Management*. Available from: http://www.dohc.ie/publications/pdf/major_emergency.pdf?direct=1. [Accessed January 2010].

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

De Vaus, D.A. (2002). "Surveys in Social Research",(5th ed), London, Routledge.

Deverell, D. 2009. Crises as Learning Triggers: Exploring a Conceptual Framework of Crisis-Induced Learning. *Journal of Contingencies and Crisis Management*, Vol 17(3), pp179 -188.

De Waal, A. 2006. Towards a comparative political ethnography of disaster prevention. *Journal of International Affairs*, Spring/Summer2006, Vol59 (2), pp.129-149.

De Witte, K. van Muijen, J. 1999. Organizational Culture, *European Journal of Work and Organizational Psychology*, Vol 8 (4), pp. 497-502.

Dreyer, S. and Ingram, D. 2008. *Standard & Poor's To Apply Enterprise Risk Analysis To Corporate Ratings*. Standard & Poor's RatingsDirect. Available from: http://www2.standardandpoors.com/spf/pdf/events/CRTconERM5908.pdf. [Accessed Jan 2010].

Dye, K. Langsett, M. 2008. A roadmap to measure and achieve enterprise operational resiliency. *Journal of Business Continuity & Emergency Planning,* Vol. 3(1), pp. 38–46.

Dynes, R. Quarantelli, E. 1977. *Organizational communications and decision making in a crisis*, University of Delaware, Disaster Research Centre, Newark, DE I 19716, Report Series, 17. Available from: http://dspace.udel.edu:8080/dspace/bitstream/19716/1264/1/RS17.pdf. [Accessed January 2010].

Eastwood,G.2008. Building the Responsive Enterprise. *Business Insights database*: Available from http://www.bi-interactive.com/index.aspx?StoryID=585203&ReportID=794&Lang=en&MainPage=renderDownload. [Accessed December 2009].

Egan, M. 2007. Anticipating Future Vulnerability: Defining Characteristics of Increasingly Critical Infrastructure-like Systems, *Journal of Contingencies and Crisis Management*, Vol 15(1), pp 4 – 17.

Elliott, D. 2009. The Failure of Organizational Learning from Crisis – A Matter of Life and Death? *Journal of Contingencies and Crisis Management*, Vol 17(3), pp. 157-168.

Elliott, D. Johnson, N. 2010. A Study of Resilience and Business Continuity Practice 2010. *Business Continuity Project Final report,* University of Liverpool Management School, p. 47.

Elliott, D. Swartz, E. and Herbane, B., 2002. *Business Continuity Management – A crisis management approach*, London: Routledge.

Elliott, D. Swartz, E. and Herbane, B., 2010. *Business Continuity Management – A crisis management approach*, (2nd ed), London: Routledge.

Ellwood, A. 2009. Using the disaster crunch/release model in building organisational resilience. *Journal of Business Continuity & Emergency Planning*, Vol 3(3), pp. 241-247.

EU Council 2008, *European Critical Infrastructure*, *Factsheet 2008*, Justice and Home Affairs Council, Luxembourg, Available from:

http://www.eurunion.org/partner/euusterror/EUCritInfrastructFactsheet-6-5-08.pdf. [Accessed September 2009].

European Commission 2010, Available from: http://ec.europa.eu/environment/emas/emasawards/awards.htm.
[Accessed February 2011].

Fink, S. 1986. *Crisis Management*, New York: AMACOM, American Management Association.

Fritzon, A. Ljungkvist, K. Boin, A. Rhinard, M. 2007. Protecting Europe's Critical Infrastructures: Problems and Prospects. *Journal of Contingencies and Crisis Management*, Vol 15(1), March 2007, pp. 30–41.

Fry, M. 2004. Service-continuity goals important. *Communications News*, Vol. 41(10), pp.48-46. Available from: http://web.ebscohost.com/ehost/detail?vid=8&hid=104&sid=49469f97-66c4-4176-

b8a9-33197e79bde0%40sessionmgr111&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=14670149. [Accessed November 2009].

GAO Reports, 1998, *Status Information: FAA's Year 2000 Business Continuity and Contingency Planning Efforts Are Ongoing*: AIMD-99-40R.pp1-6. Available from: http://web.ebscohost.com/ehost/detail?vid=6&hid=108&sid=f0413e71-1baa-47b2-8591-402f90a98ea0%40sessionmgr110&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=18224268 [Accessed October 2009].

Gallagher, M. 2003. *Business Continuity Management - How to protect your company from danger*, FT Prentice Hall, London, England: Pearson Education Limited.

Gallagher, M. 2011. Business Continuity Management 'Do you measure up'. *Continuity Central*. Available from: http://www.continuitycentral.com/selfassessment.pdf [Accessed January 2011].

Galliers, R.D. (1991) Choosing appropriate information systems research approaches: a revised taxonomy. In: *Information Systems Research: Contemporary Approaches and Emergent Traditions*, Nissen, H.-E., Klein, H.K. & Hirschheim, R. (eds), pp. 327–345. Elsevier Science Publishers, North Holland.

Ginn, R. 1992. *Continuity Planning – Preventing, Surviving and Recovering from Disaster*, Oxford, England: Elsevier Science Publishers Ltd.

Goel, S.and Butler, B. 2008. I.T. *Business Continuity Management in Large Global Corporations: Insights, issues and recommendations*. University of Pittsburgh, Joseph.M. Katz Graduate School of Business. Available from: http://iswik.org/wiki/sg/Business%20Continuity%20Management%20in%20Large%20Global%20Corporations.pdf. [Accessed November 2009].

Goodwin, B. 2005. A third of companies have no plan for ensuring business continuity*, Computer Weekly*, p15.

Gregory, D.2008. Communicating in a crisis: A risk management issue? *Journal of Business Continuity & Emergency Planning*, Vol. 3 (1), pp. 31–37.

Hamilton, D. 2007. Survive the Worst Is Your Business Ready? *Accountancy Ireland*, Vol 39 (6), pp. 42 -43.

Hemp, P. 2009. Death by information overload. *Harvard Business Review*, Vol. 87(9), pp. 82-89. Available from: http://web.ebscohost.com/ehost/detail?vid=24&hid=108&sid=a179dc34-af77-431a-a2d0-

b378ec56492b%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=43831174. [accessed February 2010].

Herbane, B. 2010. The evolution of business continuity management: A historical review of the practices and drivers. *Business History*, 52:6, pp. 978-1002.

Herbane, B. Elliot, D. and Swartz, E. 1997. Continuity and continua: Achieving excellence through business continuity planning. *Business Horizons*, (November-December), (1997): Vol 40(6), pp. 19-25.

Higgs, M. and Rowland, D. 2005. All changes great and small: Exploring approaches to change and its leadership. *Journal of Change Management*, Vol. 5(2), pp. 121-151. Available from: http://web.ebscohost.com/ehost/detail?vid=7&hid=5&sid=f593c135-32a0-4721-9c2b-9ae42b4d0311%40sessionmgr4&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=17588595. [Accessed October 2009].

Hiles, A. 2007a. An Introduction to business continuity planning *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. xix-xxvii.

Hiles, A. 2007b. Developing and implementing the written plan *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 279-314.

Hiles, A. 2007c. Awareness and training *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 315-322.

Hoffer G. Cameron, J. Lim, K. and Rivas, S. 2006. Relationships, Layoffs, and Organizational Resilience. *Journal of Applied Behavioral Science*, Vol. 42(3), pp. 300-329. Available from: http://web.ebscohost.com/ehost/detail?vid=13&hid=5&sid=58b56019-652a-4b27-966e-a0e54a4eff3f%40sessionmgr11&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=22253060. [Accessed September 2009].

Holowachuk, B. 2007. Developing an organisation-wide business continuity programme in the public sector: Case study of the Government of Manitoba, *Journal of Business Continuity & Emergency Planning,* Vol. 2 No. 1, pp. 21–32.

Horne, J. and Orr, J. 1998. Assessing behaviours that create resilient organizations. *Employment Relations Today*, 24(4), pp. 29–39.

Horne III, J. 1997. The coming age of organizational resilience. *Business Forum*, Spring/Fall97, Vol 22 (2/3/4), pp. 24-28.

Howe, J. 2007. Project initiation and management *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 122.

IBM Global Technology Services. 2009. *Getting personal with business continuity: Five critical success factors in overcoming workforce disruptions*. IBM Corp. Available from: http://www-935.ibm.com/services/ie/gts/getting_personal_with_business_continuity.pdf. [Accessed January 2010].
www.knowledgetransfer.net. Business Continuity Management (ITILv3). Available from: http://www.knowledgetransfer.net/dictionary/ITIL/en/Business_Continuity_Management.htm. [Accessed Dec 2010].

Jackson, R. 2006. Business continuity: Preparation over Prevention. *Accountancy Ireland*, Dec 2006, Vol. 38(6), pp. 51-53.

Johnson, G. Scholes, K. 2002. *Exploring Corporate Strategy*, Sixth Edition, England: Pearson Education Limited.

Kaplan, B. & Duchon, D. (1988). "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study", *MIS Quarterly*, December, pp. 571-586.

Karakasidis,K. 1997. A project planning process for business continuity, *Information Management & Computer Security*, Vol.7(8),pp 72–78.

Kello, J. 2009. How to assess your culture. *Industrial Safety & Hygiene News*, Jun 2009, Vol. 43(6), pp. 24-26.

Kelly, M. & McMullan, C. 2011, *Implementing Business Continuity Management – Sharing Good Practice from an Irish Context.* 1st International Conference on Safety and Crisis Management in the Construction, Tourism and SME Sectors (1st CoSaCM)

Khazanchi, D. and Munkvold, B. 2000. *Is information system a science?* An inquiry into the nature of the Information Systems discipline. SIGMIS Database, 31(3), pp.24-42.

Klinec, I. 2004, *Strategic Thinking in the Information Age and the Art of Scenario Designing*, Institute for Forecasting. Slovak Academy of Sciences. Available from: http://www.futurologia.sk/strategicthinking.ppt. [Accessed October 2009].

Kjærgaard, A. 2009. Organizational Identity and Strategy. *International Studies of Management and Organization*, Vol. 39(1), pp. 50–69.

Koch, R. 2004. Best practices in business continuity. *Communications News*, Vol. 41(11), Nov 2004, p 24.

Kotnour, T. 2009. Putting Culture to Work in Our Organizations. *Engineering Management Journal,* June 2009,Vol. 21(2), p 1-2.

Lagadec, P. 2009. A New Cosmology of Risks and Crises: Time for a Radical Shift in Paradigm and Practice. *Review of Policy Research*, Jul 2009, Vol. 26(4), pp. 473-486.

Laliberte, B. 2007. How Disaster-Tolerant Is Your Company? *Business Communications Review*, Vol. 37(9), pp.44-48. Available from: http://web.ebscohost.com/ehost/detail?vid=20&hid=104&sid=63e8c31c-07ad-475d-b36c-. [Accessed November 2009].

LaPorte, Todd R. 1996. High Reliability Organizations: Unlikely, demanding, and at risk. *Journal of Contingencies and Crisis Management,* Vol. 4, p. 63.

LaPorte, T R. and Consolini, P. 1991. Working in Practice But Not in Theory: Theoretical Challenges of High-Reliability Organizations. *Journal of Public Administration Research and Theory*, Vol. 1, pp. 19–47.

Lengnick-Hall C. and Beck T. 2008. Resilience Capacity and Strategic Agility: Prerequisites for Thriving in a Dynamic Environment, The University of Texas at San Antonio, College of business. Available from: http://business.utsa.edu/wps/mgt/0059MGT-199-2009.pdf. [Accessed July 2010].

Lindstedt, D. 2007. Grounding the discipline of business continuity planning: What needs to be done to take it forward? *Journal of Business Continuity & Emergency Planning*, Vol. 2 (2), pp. 197–205.

Lodge, M. 2009. The Public Management of Risk: The Case for Deliberating among Worldviews. *Review of Policy Research*, Vol. 26(4), pp. 395-408. Available from: http://web.ebscohost.com/ehost/detail?vid=5&hid=105&sid=b6b67651-5996-4cde-9f0e-8fca1e4929e9%40sessionmgr112&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=41888939. [Accessed December 2009].

Luthans, F. 2002. *Organizational Behaviour*, New York: McGraw-Hill.

Mallak, L. 2009. Putting culture to work in our organizations. *Engineering Management Journal*, Vol 21(2), pp. 1-2. Available from: http://web.ebscohost.com/ehost/detail?vid=3&hid=108&sid=a179dc34-af77-431a-a2d0-b378ec56492b%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=43605658#db=buh&AN=43605658. [Accessed October 2009].

Massoud, A. and Horowitz, B. 2008. Toward Agile and Resilient Large-Scale Systems: Adaptive Robust National/International Infrastructures. *Global Journal of Flexible Systems Management*. Vol. 9(1), pp. 27-39. Available from: http://web.ebscohost.com/ehost/detail?vid=8&hid=108&sid=38e70d3f-627f-4625-

832c-afb2bbe916fc%40sessionmgr110&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=35457838. [Accessed January 2010].

Marshall, J. Smith, S. and Buxton, S. 2009. Learning organisations and organisational learning: What have we learned? *Management Services*; Autumn2009, Vol. 53(3), pp. 14-19. Available from: http://web.ebscohost.com/ehost/detail?vid=6&hid=108&sid=378db3e3-ded7-4c3e-b67b-dd7025a295e5%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=45060956. [Accessed December 2009].

Maxwell, J. 1996. *Qualitative research design: An interactive approach*, Thousand Oaks, CA: Sage.

McLoughlin, R. 2008. What one must know about achieving BS25999-2 certification, *Journal of Business Continuity & Emergency Planning,* Vol. 3(2), pp. 105–111.

Mitroff, I. 2001. *Managing Crises Before They Happen: What Every Executive and Manager Needs to Know About Crisis Management*, New York: Amaco.

Mitroff,I. 2005. Lessons from 9/11, Are companies better prepared today?. *Technological Forecasting & Social Change*, Vol 72,pp 375–376.

Mitroff, I. Pauchant, T. Finny, M. and Pearson, C. 1989. Do (some) organizations cause their own crisis? Culture profiles of crisis-prone versus crisis-repaired organizations. *Organization & Environment,* 3(4), pp 269-83.

Mitchell, V (1996). "Assessing the reliability and validity of questionnaires: an empirical example", *Journal of Applied Management Studies*, Vol 5:2, pp. 199-207.

Moynihan, D. 2009. The Network Governance of Crisis Response: Case Studies of Incident Command Systems. *Journal of Public Administration Research & Theory*, Vol. 19(4), pp. 895-915. Available from: http://web.ebscohost.com/ehost/detail?vid=5&hid=9&sid=b8d9d6ab-7a81-478e-a449-4959a48817d7%40sessionmgr14&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=44587011. [Accessed January 2010].

Myers, K. 2006. *Business Continuity Strategies: Protecting Against Unplanned Disasters*, Hoboken, New Jersey: John Wiley & Sons, Inc.

NFPA 1600. 2010 *Standard on Disaster/Emergency Management and Business Continuity Programs*, National Fire Prevention Authority. Available from: http://www.nfpa.org/assets/files/pdf/nfpa16002010.pdf. [Accessed January 2011].

National Organisational Resilience Framework workshop. 2007. "*The Outcomes: Business Continuity Management Information Exchange.".* Available from: http://www.bcmie-australia.org/Download/Final%20Report.pdf.

[Accessed November 2009].

Nolan, R. 1979. Managing the crises in data processing. *Harvard Business Review*, Vol. 57(2), pp. 115-116. Available from: http://web.ebscohost.com/ehost/detail?vid=12&hid=5&sid=f593c135-32a0-4721-9c2b-9ae42b4d0311%40sessionmgr4&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=3867671. [Accessed November 2009].

Nollau, B. 2009. Disaster Recovery and Business Continuity. *Journal of GXP Compliance,* Summer 2009, 13(3), pp. 51-59.

O'Hehir, M. 2007. What is a business continuity planning (BCP) strategy *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 27-45.

O'Leary, Z. (2004). *The Essential Guide to Doing Research*. London: Sage Publications.

Oldfield, R. 2008a. Organizational resilience. *Continuity Central*. Available from:

http://www.continuitycentral.com/feature0618.html. [Accessed November 2009].

Oldfield, R. 2008b. So what is resilience and what benefits does it offer?. Available from:
http://www.organisationalresilience.com.au/files/orgresilaug08.pdf.
[Accessed November 2009].

Oriesek, D. Schwarz, J. 2008. *Business War gaming*, Burlington, USA: Ashgate Publishing Company.

Panko, R. 1987.Directions and issues in end user computing.INFOR, Vol. 25(3), pp.181-197. Available from: http://web.ebscohost.com/ehost/detail?vid=14&hid=5&sid=f593c135-32a0-4721-9c2b-9ae42b4d0311%40sessionmgr4&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=6284293. [Accessed October 2009].
Pas 56. 2003. *An Overview from automata, 2005*. Available from: http://www.automataservices.com/PAS%2056%20Overview1.doc.
[Accessed October 2009].

Pearson,C. and Clair, J. 1998. Reframing Crisis management. *Academy of Management Review*. Vol 23(1), pp. 59-76.

Perman, G. 2009. Why Succession Management Matters. CIO Insight, Issue 103, pp. 34-36. Available from: http://web.ebscohost.com/ehost/detail?vid=16&hid=103&sid=3e294d01-2636-4d8f-8025456804bf6b5%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=38423726.
[Accessed January 2010].

Pollard, C. and Cater-Steel, A. 2009. Justifications, Strategies, and Critical Success Factors in Successful ITIL Implementations in U.S. and Australian Companies: An Exploratory Study. *Information Systems Management*, Vol. 26(2), pp.164-175. Available from: http://web.ebscohost.com/ehost/detail?vid=10&hid=105&sid=b6b67651-5996-4cde-9f0e-8fca1e4929e9%40sessionmgr112&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=37604191. [Accessed November 2009].

Preimesberger, C. 2009. Unfettered data growth challenges business continuity technology. *eWeek*, Vol 26(6), pp. 16-18. Available from: http://web.ebscohost.com/ehost/detail?vid=4&hid=108&sid=38e70d3f-627f-4625-832cafb2bbe916fc%40sessionmgr110&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=37334477#db=buh&AN=37334477. [Accessed November 2009].

Price, R.:2009. Following Strategies less travelled. *Industrial Engineer*, Vol.41(3), pp36-39. Available from: http://web.ebscohost.com/ehost/detail?vid=17&hid=104&sid=63e8c31c-07ad-475d-b36c-9104883900a2%40sessionmgr114&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=37803066. [Accessed October 2009].

Rake, M. and, Grayson, D. 2009. Embedding corporate responsibility and sustainability – everybody's business. *Corporate Governance*,VOL 9(4), pp. 395-399.

Remenyi, D. Williams, B. Money, A. and Swartz, E. 1998. Doing Research in Business and Management, An Introduction to Process and Method, London: Sage.

Rhinard, M. 2009. European Cooperation on Future Crises: Toward a Public Good. *Review of Policy Research*; Vol. 26(4), pp. 439-455.

Riolli, L. and Savicki, V. 2003. Information system organizational resilience. *International Journal of Management Science*, Omega, 31, Elsevier Science Ltd, pp. 227-233.

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

Rossing von, R. 2007. BC Audit *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, p. 339.

Roux-Dufort, C. 2007, Is Crisis Management (Only) a Management of Exceptions?. *Journal of Contingencies and Crisis Management*, Vol 15(2), pp 105 – 114.

Rugg G. & Petre M. 2007. *A gentle guide to research methods*. Open University Press.

Sandin, P. 2009. Approaches to Ethics for Corporate Crisis Management. *Journal of Business Ethics*, Vol 87(1), pp 109–116. Available from: http://proquest.umi.com/pqdweb?index=4&did=1736409491&SrchMode=3&sid=3&Fmt=6&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1278325158&clientId=28085&aid=1. [Accessed January 2010].

Saunders, Lewis and Thornhill, 2007. *Research Methods for Business Students*, Harlow, Essex, England: Pearson Education Limited.

Schild, P. 2009. Improving Risk Management: Process and Culture. *Financial Executive*, Vol. 25(4), p. 55. Available from: http://web.ebscohost.com/ehost/detail?vid=4&hid=108&sid=e568ce87-fec5-4359-8b37-757dba821266%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=41228230. [Accessed January 2010].

Schulman, P. and Roe, E.2007, Designing Infrastructures: Dilemmas of Design and the Reliability of Critical Infrastructures. *Journal of Contingencies and Crisis Management*, Vol 15(1), pp 42 – 49.

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

Sevcik, P. 2007. Can The 'Net Support Business Continuity? *Business Communications Review*, Vol. 37(1), pp. 10-12. Available from: http://web.ebscohost.com/ehost/detail?vid=19&hid=103&sid=3e294d01-2636-4d8f-8025-1456804bf6b5%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=24209626. [Accessed November 2009].

Seville, E.2009. *The Goal of Resilient Organisations*. Brisbane, Australia: 3rd Annual Business Continuity Summit 2009, pp. 24-26. Available from: http://ir.canterbury.ac.nz/bitstream/10092/2963/1/12618127_BCI%20Summit%20-%20Seville.pdf. [Accessed November 2009].

Shaluf, I.M. 2007. An overview on the technological disasters. *Disaster Prevention and Management,* Vol. 16(3), pp. 380-390.

Shankar S, 2008. An alternative methodology for business impact analysis in a service-oriented industry, *Journal of Business Continuity & Emergency Planning*,Vol. 3(2), pp. 124–131.

Shaw,G. 2005. *Business Crisis and Continuity Management*, The George Washington University Institute for Crisis, Disaster, and Risk Management, Available from: http://www.gwu.edu/~icdrm/publications/ShawTextbook011105.pdf. [Accessed December 2009].

Sheffi, Y. 2007. *The Resilient Enterprise*, Cambridge, Massachusetts: The MIT Press.

Sheffi Y. and Rice Jr, J. 2005. Building the Resilient Enterprise, *MIT Sloan Management Review*, Fall 2005, Vol 42(1).

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*, Vol. 2(3), pp. 221-239.

Sikich, G. 2003. Integrated business continuity: maintaining resilience in uncertain times, Oklahoma, USA: PennWell.

Simpson, D. 2008. Disaster preparedness measures: a test case development and application. *Disaster Prevention and Management*, Vol. 17(5), pp. 645-661.

Sisk, M. 2009. The Tweet That Saved the Bank. *Bank Technology News*, Vol. 22(8), pp. 25-25.

Skelton, P. 2007, Business continuity and supply chain management: How to manage logistical operations in the event of an interruption or emergency, *Journal of Business Continuity & Emergency Planning*, Vol. 2 (1), pp. 13–20.

Smith D. 2005. Business (not) as usual: crisis management ,service recovery and the vulnerability of organisations. *Journal of Services Marketing,* Vol 19(5), 2005, pp. 309–320.

Smith, M. and Sherwood, J. 1995. Business Continuity Planning, *Computers and Security*, 14(1), pp. 14-23.

Smith, M and Shields, P-A. 2007. Strategies for IT and communications *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, p. 205.

Somers, S. 2009. Measuring Resilience Potential: An Adaptive Strategy for Organizational Crisis Planning. *Journal of Contingencies and Crisis Management*,Vol 17(1), pp 12 -23.

Somers, S. and Svara J. 2009. Assessing and Managing Environmental Risk: Connecting Local Government Management with Emergency Management. *Public Administration Review*, Mar/Apr2009, Vol. 69(2), pp.181-193.

Spigener, J. 2009. Can you recognize "exposure creep"? *Industrial Safety & Hygiene News*, Jun 2009, Vol. 43(6), pp. 44-46.

Stucke, C. Straub, D. and Sainsbury, R. 2008. Business Continuity Planning and the Protection of Informational Assets. *IN:* Straub, D. Goodman, S. Baskerville, R.(ed's). *Information Security Policies and Practices*, Armonk, NY: M.E. Sharpe, pp.152-172. Available from:
http://www.cis.gsu.edu/~dstraub/Present/2008/bcppaper.pdf.
[Accessed November 2010].

Sun Tzu. "*The Art of War*", 544-496 BC.

Swartz, E. Elliott, D. and Herbane, B. 1995. Out of sight, out of mind: the limitations of traditional information systems planning. *Facilities*, Vol 13(9/10), pp. 15–21. Available from:
http://www.ingentaconnect.com/content/mcb/069/1995/00000013/F0020009/art00003
. [Accessed October 2009].

Swiss Federal Banking Commission (SFBC). 2007. *Recommendations for Business Continuity Management (BCM)*. p. 4. Available from: www.swissbanking.org/en/11107_e.pdf. [Accessed December 2010].

Taleb, N. 2007. *The Black Swan*, London, England: Penguin Books.

Thornton, G.2008, An innovative, flexible and workable business continuity plan: Case study of the Australian Customs Service Cargo BCP, *Journal of Business Continuity & Emergency Planning*, Vol. 3(1), pp. 47–54.

Turner, B. 1976. The organizational and inter-organizational development of disasters. *Administrative Science Quarterly*, 21, pp. 378-89.

United States General Accounting. 1999, *Year 2000 Computing challenge*, OfficeGAO/AIMD-00-11, Available from: http://cryptome.org/fbi-y2ked.htm
[Accessed December 2009]

Van Eeten, M. and Bauer,J. 2009, Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications, *Journal of Contingencies and Crisis Management* Vol17(4), pp 221 - 232

Vaid, R. 2008. How are operational risk and business continuity coming together as a common risk management spectrum?. *Journal of Business Continuity & Emergency Planning*, Vol. 2(4), pp. 330–339.

Viner, P. 2007. Operational Risk Management *IN:* Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*. Second Edition, England: John Wiley & Sons Ltd, pp. 83-96.

Vizard, M. 2008. Why there's no business continuity. *Baseline*, Sep 2008, Issue 88, p 18. Available from: http://web.ebscohost.com/ehost/detail?vid=6&hid=108&sid=38e70d3f-627f-4625-832cafb2bbe916fc%40sessionmgr110&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=34222133. [Accessed January 2010].

Wachtendorf, T. 2009. Trans-System Social Ruptures: Exploring Issues of Vulnerability and Resiliency. *Review of Policy Research*, Vol. 26(4), pp. 379-393. Available from: http://web.ebscohost.com/ehost/detail?vid=15&hid=105&sid=b6b67651-5996-4cde-9f0e-8fca1e4929e9%40sessionmgr112&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=41888940. [Accessed December 2009].

Wack, P. 1985. Scenarios: uncharted waters ahead. *Harvard Business Review*, September-October 1985, pp. 73-89.

Wester, M. 2009. Cause and Consequences of Crises: How Perception Can Influence Communication. *Journal of Contingencies and Crisis Management*, Volume 17(2), pp 118-125.

Whittet, L**.** 2008. Operational risk management and business continuity. *Continuity Central*, Available from: http://www.continuitycentral.com/feature0606.html. [Accessed January 2010].

Woodman, P and Kumar, V. 2009. *A Decade of Living Dangerously*, Chartered Management Institute. Available from: http://www.cabinetoffice.gov.uk/media/153711/cmibcm_2009.pdf. [Accessed January 2010].

World Economic Forum. 2008. *Global Risks 2008*. Available from: http://www.weforum.org/pdf/globalrisk/Risk08.pdf. [Accessed October 2009].

World Economic Forum. 2009. *Global Risks 2009*. Available from: http://www.weforum.org/pdf/globalrisk/globalrisks09/global_risks_2009.pdf. [Accessed Ferruary 2010].

Wright, C. and Suh, C-S. 2009. If at first you don't succeed: globalized production and organizational learning at the Hyundai Motor Company. *Asia Pacific Business Review*, Vol. 15(2), pp. 163-180. Available from: http://web.ebscohost.com/ehost/detail?vid=3&hid=105&sid=b6b67651-5996-4cde-9f0e-8fca1e4929e9%40sessionmgr112&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=38028555. [Accessed December 2009].

Youngblood, M. D. 2000. Winning cultures for the new economy. *Strategy & Leadership*, 28(6), pp. 4-10.

Zalud, B. 2008. Carrying On After a Disaster. *Security: For Buyers of Products, Systems & Services*, Vol. 45 (7), pp.12-14. Available from: http://web.ebscohost.com/ehost/detail?vid=15&hid=108&sid=a179dc34-af77-431a-a2d0-b378ec56492b%40sessionmgr113&bdata=JkF1dGhUeXBlPWNvb2tpZSxpcCxhdGhlbnMmc2l0ZT1laG9zdC1saXZl#db=buh&AN=33303709. [Accessed February 2010].

Zollo, M. Minoja, M. Casanova, L. Hockerts, K. Neergaard, P. Schneider, S. and Tencati, A. 2009.Towards an internal change management perspective of CSR: evidence from project RESPONSE on the sources of cognitive alignment between managers and their stakeholders, and their implications for social performance. *Corporate Governance*, Vol 9(4), pp. 355-372.

APPENDICES

APPENDIX A

Survey Cover letter and questionnaire:

Business Continuity Management Survey

Date: April 2009

Dear ,

As part of my Masters in Business Continuity Management at Dublin City University Business School, I am researching how Business Continuity Management has evolved in medium to large Irish enterprises between 2004 and 2009. This work is being completed with Dr Caroline McMullan.

I was delighted when your organization responded to my survey in 2004 and I am hoping that you will assist me once again. The success of my research relies on getting responses from the same organizations five years later.

I am asking you to look over the survey attached and, if you choose to do so, participate in the research. It should take you about 15 minutes to complete. The survey does not require you to give your name or any information that might identify you. Information compiled from the questionnaire will be reported in my Masters thesis and all individuals and organizations will remain anonymous. All completed questionnaires will be stored under lock and key at my home until I complete my degree when they will be destroyed.

The study is being conducted by me in a personal capacity. You do not have to participate in the study if you do not wish to do so.

I would like to thank you for taking the time to read this letter and hope can find the time to assist me with my research.

Yours faithfully

David Garrett
3 Willow Park,
Millfarm,
Dunboyne,
Co Meath.

Introduction to the Survey

This survey asks you questions about Business Continuity Management. The survey should take no more than 15 minutes to complete. Please choose the answer that most closely reflects your feeling about each statement.

Thank you for taking the time to complete the survey.

SECTION 1: Business Continuity Management --

1. How would you characterise the extent of the disruption caused to your organization by the following events?

[Please tick ONE box in each row only]

	Severe	Serious	Modest	Non-existent	Don't know
Increased terrorist activity	□	□	□	□	□
Power failures	□	□	□	□	□
Postal strikes	□	□	□	□	□
Extreme summer temperatures	□	□	□	□	□
Computer viruses/bugs	□	□	□	□	□

2. Which, if any, of the following has your organization experienced in the past year? *[Please tick as applicable]*

Loss of site	□
Loss of telecommunications	□
Loss of IT capacity	□
Supply chain disruption	□
Loss of skills	□
Environmental liability	□
Loss of people	□
Employee health and safety scare	□
Floods/ high winds	□
Customer health/ product safety issue	□
Fire	□
Pressure group protest	□
Terrorist damage	□
Damage to corporate image/ reputation/ brand	□
Military conflict	□
Negative publicity/ coverage	□

Other

____

3 In your opinion, how important is Business Continuity to senior management within your organization? *[Please tick ONE box only]*

Very important □
Important □
Neutral □
Not important □

4. What is the main driver for change to your organizations approach to Business Continuity Management?

[Please tick ONE box only]

Corporate Governance □
Central government □
Regulators □
Insurers □
Existing customers □
Potential customers □
Auditors □
Investors □
Suppliers □
Don't know □
Has not looked at BCM □

Other______________________________

5. Has your organization been asked to provide evidence of Business Continuity Management by any of the following bodies and groups?

[Please tick as applicable]

Central government □
Insurers □
Regulators □
Banks □
Other external funding bodies □
Potential customers □
Existing customers □
Auditors □
Credit rating agencies □
No external requests □

Other____

6. From where does your organization obtain information about Business Continuity Management?

7. Does your organization have a Business Continuity Plan?

Yes	□	
No	□	***[Go to Question 20]***
Don't know	□	***[Go to Question 20]***

8. Which of the following does your Business Continuity Plan cover …?

[Please tick as applicable]

Loss of site	□
Loss of IT capacity	□
Loss of skills	□
Lose of people	□
Floods/ high winds	□
Fire	□
Terrorist damage	□
Military conflict	□
Loss of telecommunications	□
Supply chain disruption	□
Environmental liability	□
Employee health and safety scare	□
Customer health/ product safety issue	□
Pressure group protest	□
Damage to corporate image/ reputation/ brand	□
Negative publicity/ coverage	□

Other ________________________________

9. How frequently is your Business Continuity Plan exercised?

[Please tick ONE box only]

At least every 3 months	□	
At least every 6 months	□	
Approx once a year	□	
Approx every 2 years	□	
Approx every 3 years	□	
Not at all	□	**[*Go to Question 12]***

10. Has a Business Continuity plan exercise revealed any shortcomings in its effectiveness, and have these been addressed?

[Please tick ONE box only]

Yes, but not addressed	□
Yes, have been addressed	□
No	□
Don't know	□

11. To what organizational level are your Business Continuity plans exercised?
[Please tick ONE box only]

IT recovery only □
Workplace/site recovery □
Business unit □
Organization-wide □
Board level scenario □
Don't know □

12. Within your organization who is …

a) responsible for Business Continuity Management?
b) involved in creating the Business Continuity Plan?
c) the owner of the plan in order for it to be effectively implemented?

	a) responsible for	b)create plan	c)own plan
Board level	□	□	□
Senior management	□	□	□
Middle management	□	□	□
Business Continuity Manager	□	□	□
Operational staff	□	□	□

Other ____

13. Are you familiar the BS 25999 standard that guides Business Continuity Management activities?

Yes □
No □

14. Does your organization use BS 25999?

Yes □
No □

15. To whom is your organization's Business Continuity capability communicated? *[Please tick as applicable]*

Regulators □
The investment community □
Insurance companies □
Shareholders □
Senior management / Board □
Employees □
Local community □
Suppliers □
Customers □
Don't know □
Other ____

16. **Which functions in your organization are included in your Business Continuity Plans?** *[Please tick as applicable]*

Production/ manufacturing □
Finance □
Sales □
Marketing □
Purchasing □
Outsourcing □
Human resources □
Information technology □
Facilities management □
Security □
Public relations □
Other ______________________________

17. **Does your organization:**

a) **outsource any of its facilities / services?**
[Please tick ONE box only]

Yes □
No □
Not applicable □

If 'Yes' does it

b) **require its outsource suppliers to have Business Continuity Plans?**
[Please tick ONE box only]

Yes □
No □
Not applicable □

18. **If your organization insists on its outsource suppliers having Business Continuity Plans, how are these verified?**
[Please tick as applicable]

Statement from suppliers □
Examination of Business Continuity Plans □
Involvement in exercise □
Involvement in Business Continuity development □

19. **Will your 2009 budget associated with Business Continuity Management …?**

[Please tick one]

Increase substantially □
Increase marginally □
Remain the same □
Decrease □
Don't know □

SECTION 2: Power Management

20. Has your organization experienced any power outages in the past year?
Yes □
No □

21 a Does your Business Continuity Plan cover power outages specifically?
Yes □
No □

21b. Does your organization have its own generator?
Yes □
No □

22. Does your organization have its own Uninterrupted Power Supply (UPS)?
Yes □
No □

23. Do your outsource suppliers having generators & UPS capabilities to ensure their services, and if so how do you verify that they do?
[Please tick as applicable]

Statement from suppliers □
Examination of Business Continuity Plans □
Involvement in rehearsals □
Involvement in Business Continuity plan development □

SECTION 3: Information Technology Service Management (ITSM)

24. Does your organization operate or follow any of the following ITSM approaches? *[Please select one]*

ITIL □
COBIT □
Capability Maturity Strategy □
Microsoft Operations Framework (MOF) □
Other ______________________________

25. Does your organization use any of the following ITSM tools?

[Please select one]

Microsoft SCCM/SCOM □
HP Openview □
BMC Patrol □
IBM Tivoli □
CA UniCentre □

Other ______________________________________

26. If your organization is considering implementing ITSM in 2009, what is the key driver? *[Please select one option only]*

Improve service levels for the Business □
Improve IT internal processes □
Reduce the costs of service provision □

Other ______________________________________

SECTION 4: Classification

27. What is your managerial level?

Director □
Senior manager □
Middle manager □
Junior manager □
Other ______________________________

28. What is the status of your organization? *[Please tick ONE box only]*

Private limited company □
Public sector □
Partnership □
Public limited company □
Owner managed / Sole trader □
Other ________________________________

29. In which industrial sector is your organization? *[Please tick ONE box only]*

Construction/ engineering □
Utilities □
Professional/ consultancy □
Manufacturing/production □
Public administration/ government □
Business services □
Distribution/ transport □
Retail/ wholesale □
Education/ training □

Banking/ insurance/ finance □

Health □
Leisure □
Emergency services □
Other ______________________________

30. What is your organization's area of operation? *[Please tick ONE box only]*

Local □
Regional □
National □
International □

31. In which area is your organization's principal office based?

[Please tick ONE box only]

Leinster □
Munster □
Ulster □
Connaught □

32. What is the annual turnover of your organization?

Up to €10m □
€11m - €100m □
€101m - €500m □
Over €500m □

33. How many employees does your organization have in Ireland?

51 - 100 □
101 - 200 □
201 - 1,000 □
1,001 - 5,000 □
5,001 - 10,000 □
Over 10,000 □

Any comments you have would be greatly appreciated.

THANK YOU FOR YOUR TIME AND ASSISTANCE. ALL REPLIES WILL BE TREATED IN CONFIDENCE AND WILL NOT BE ATTRIBUTABLE IN ANY WAY
Thank you again for your help!

APPENDIX B

Interview Schedule

<u>Qualitative questions for interviews</u>

Q1(a) In the organizations which I have studied responsibility for BCM seems not to sit at Director level. Does this match your view of BCM?

1(b) Why do you think this is so?

Q2 (a) Is BCM a high priority for senior management?

(b) If not, why do you think this is so?

Q3 What would you say are the incidents most likely to disrupt an organization and trigger the need for BCM?

Q4 Those surveyed identified the following as the top four incidents their organizations experienced in the past year?

1. Loss of telecommunications
2. Loss of people
3. Loss of skills
4. Loss of IT capacity

Why do you think organizations are vulnerable in these areas?

Q5 My study revealed that the perceived threat from terrorist activity has dropped over the past 5 years – why do you think this is so?

Q6 (a) Have large organizations improved their business processes over the past 5 years?

(b) If yes, has this improved their resilience?

Q7 (a) Have large organizations increased their investment in BCM over the past 5 years?

(b) If yes, has this improved resilience?

Q8 Do you think central government has taken a keener interest in the BCM capabilities of organizations over the past 5 years?

Q9 Have regulators taken a keener interest in the BCM capabilities of organizations over the past 5 years?

Q10 From what sources do you think organizations get their information on BCM?

Q11 Do you think government agencies are used as a source of BCM information?

Q12 Within organizations, who do you think is usually:

- responsible for Business Continuity Management?
- involved in creating the Business Continuity Plan?
- the owner of the plan and responsible for implemented?

Q13 Has BS25999 had a wide/significant impact on BCM in large organizations?

Q14 To whom are organizations most likely to communicate their BC capabilities?

Regulators
The investment community
Insurance companies
Shareholders
Senior management / Board
Employees
Local community
Suppliers
Customers
Don't know
Other *(please specify)*

Q15 (a) Are more organization insisting on their outsource suppliers having Business Continuity Plans now than in the past?

(b) If yes, how do you think these are verified?

One of the issues I specifically explored in my study was power supply.

Q16 Do you think most large organizations have their own generators so that power outages will not materially affect their business?

Q17 Do large organizations feel the power supply to their organization is reliable?

Q18 Are some large organizations willing to accept the risks associated with power outages rather than invest in a backup power supply?

Q19 Is BCM still focused on IT and Communications, as was the case in the past?

Q20 How frequently do you think organizations exercise their BC plans?

Q21 Finally, what do you feel could be done to increase the uptake in BCM in large Irish organizations?