Determining the Critical Success Factors of an Effective Business Continuity / Disaster Recovery Program in a Post 9/11 World: a Multi-Method Approach

Michael Barbara

A Thesis
in
The John Molson School of Business

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science
at Concordia University
Montreal, Quebec, Canada

August 2006

Library and
Archives Canada

Published Heritage
Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et
Archives Canada

Direction du
Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-20809-0
Our file Notre référence
ISBN: 978-0-494-20809-0

ABSTRACT

Critical Success Factors in Implementing an Effective Business Continuity / Disaster Recovery Program in a Post 9/11 World: a Multi-Method Approach

Michael Barbara

In a society where individuals and corporations have become increasingly reliant upon information technology (IT), many have experienced or witnessed the devastation that occurs when an IT disaster strikes. As businesses increasingly rely on data, information and technology, new threats are constantly emerging that affect all corporations. Several authors agree that being well prepared is more than conforming, it is also necessary (Hawkins, Yen *et al.,* 2000; Williams, 2002; Botha and Von Solms, 2004).

Business continuity and disaster recovery (BC/DR) are strategies implemented to increase the likelihood of effectively recovering business functions from major disaster. This research project aims to fulfill two key objectives. First, this project will examine whether the ranking of critical success factors (CSFs) for implementing a BC/DR program have changed from previous research, specifically subsequent to the events of September 11th, 2001 (9/11). Second, this study will attempt to further increase contribution to the academic and practitioner communities by outlining several CSFs not referenced within previous research.

Using a multi-method approach, a qualitative analysis of 11 interviews was conducted and contrasted to results carried out through a quantitative analysis of 52 respondents through a survey questionnaire. After careful analysis of quantitative and qualitative results, four sets of CSFs were proposed and supported: BC/DR intrinsic factors, personnel requirements, analysis process and managerial issues. Surprisingly, extrinsic factors, although still required in a BC/DR initiative, have lost the lustre of the days when storage, applications and data dominated over people and processes. In essence, it was shown that the propositions formulated were confirmed, partially or fully, regarding such issues as impacts stemming from 9/11, new CSFs emanating since previous research and the aforementioned existence of a reduced set of CSFs. In addition, analyses comprised a quantitative review of the interviews, descriptive statistics and exploratory analysis using SPSS. Consequently, conclusions were derived between and within results from these types of analyses, implications to academics and practitioners suggested and future research proposed.

ACKNOWLEDGEMENTS

I would like to express my deepest thanks to all who have helped and supported me throughout this arduous yet worthwhile academic journey in accomplishing what I thought was at one point unrealizable. Having taken a much needed health sabbatical and pursuing my studies on a part-time basis, a constant flow of support and encouragement was truly needed in completing my degree within five years.

At first, a special thank you to my thesis supervisor, Dr. Kevin Laframboise, cannot go unmentioned. A constant source of support and knowledge throughout the whole thesis process, his patience and perseverance were indeed his virtues, and my prayers are with him as he is convalescing in the hospital as of the defense of this thesis.

In addition, my thesis committee members, Dr. Anne-Marie Croteau, Dr. El-Sayed Abou-Zeid and Dr. Rustam Vahidov, deserve much needed acknowledgement in my thesis work. Their advice was much needed at times and their knowledge and expertise within the IS field is well appreciated. Special mention also goes to Ms. Heather Thomson, her constant support and encouragement getting me through the tough and rough times.

To the interviewees who took time out of their much hectic schedules in order to meet and answer my questions and the survey participants who answered the questionnaire, I am truly indebted to you all.

Lastly, to my loving immediate family (Essa, Noha, and Paul), my Aunt Laure, relatives, friends and co-workers, no words can describe the gratitude that I owe each one of you. You have been there through tough and good times, always reminding me that I would be able to get through this and be proud of my achievements, of which I truly am.

LIST OF TABLES

LIST OF APPENDICES

I. INTRODUCTION

In a society where individuals and corporations have become increasingly reliant upon information technology (IT), many have experienced or witnessed the devastation that occurs when an IT disaster strikes. As businesses increasingly rely on data, information and technology, new threats are constantly emerging that affect all corporations (Booker, 2004; Castillo, 2004). Several authors agree that being well prepared is more than conforming, it is also necessary (Hawkins, Yen *et al.*, 2000; Williams, 2002; Botha and Von Solms, 2004). Regarding natural catastrophes, the U.S. Federal Emergency Management Agency (FEMA) report on their website that 1307 major disasters occurred in the United States alone between 1972 and 2001 FEMA, (2001). Natural and man-made disasters abound and new threats are constantly being mitigated. From floods to malicious computer viruses, no individual, corporation or entity is immune to the havoc and chaos inflicted when disaster strikes.

How are such events being mitigated? Business continuity (BC) and its subset, disaster recovery (DR), are contingency measures ensuring corporate recovery of business functions in the event of a disaster (Hood, 2005). Throughout the years, it has been proven that implementing such corporate initiatives will increase the chances of a faster and more efficient recovery (Wong, Monaco *et al.*, 1994; Karakasidis, 1997; Chow, 2000). Despite this fact, many corporations are unaware of the factors that need to be in place before implementing a BC or DR program (Cale and Dye, 1998).

Numerous studies have outlined the severity of the consequences stemming from disasters and have created an urgent need for corporations to "be prepared" (Arend 1992; Lee and Ross, 1995; Davis, 2004; Hood, 2005). Empirical studies (Vijayaraman and Ramakrishna, 1993; Iyer and Bandyopadhyay, 2000; Botha and Von Solms, 2004) and practitioner reports (Moore, 1995; Lethbridge, 2001; Bielski, 2003) have frequently demonstrated that losses in profit, competitive advantage, corporate image, productivity and market share are at stake if contingency measures are not properly implemented. Corporations unable to quickly recover will eventually see many of their customers switch, shareholders sell, suppliers stopping to furnish products and a loss of overall competitiveness. It is the ability to mitigate the likely effects of disasters that differentiate corporations that can quickly recover and likewise survive many years thereafter from those that fail (Paradine, 1995; Carlson and Parker, 1998; Chow, 2000; Clifton, 2000).

Disaster preparedness has taken on much greater significance since the days of plain data backup to disk and offsite storage (Rosenthal and Sheiniuk,1993; Hawkins, Yen *et al.*, 2000; AT&T, 2004). Worldwide sales of IT security and BC products and services will surpass $150 billion by 2006 (D'Antoni, 2003). Taking a "proactive approach" (Lee and Ross, 1995; Hawkins, Yen *et al.,* 2000; Sun, 2004) to BC and DR is the only viable method of ensuring a quick and effective recovery from possible threats in today's rapidly changing environment.

Objectives

Information technology, in all functional areas of business, has amplified the need for effective recovery strategies (Hawkins, Yen *et al.*, 2000). As well, it has become a top priority in many organizations (Lee and Ross, 1995). Business continuity and disaster recovery (BC/DR) strategies are implemented to increase the likelihood of effectively recovering business functions from major disaster. Several studies demonstrated that corporations having a BC and/or DR plan in place prior to the September 11th, 2001 attacks (9/11) recovered more efficiently and quickly than those that did not (Weiner, 2001; Castillo, 2004; Mendoza, 2004).

Despite this, many corporations are unaware of the factors that need to be in place before implementing a BC/DR program. Vijayaraman & Ramakrishna (1993) report that there is no shortage of reports on DR planning. However, the authors emphasize that many of these reports are in trade publications, are prescriptive in nature, detailing steps to be taken to avoid or prevent disasters. They state that empirical studies identifying the actual practices in businesses with regards to disaster preparedness are almost non-existent. Similarly, several authors deplore the lack of rigorous BC/DR studies (Heikkinen and Sarkis, 1996; Nelson, 2000; Chow, 2000; Botha and Von Solms, 2004), emphasizing that existing literature is geared towards the practitioner (Vijayaraman and Ramakrishna, 1993; Chow, 2000). As such, it would appear that the events of 9/11 have not stimulated much scientific research to rigorously study BC/DR issues. Hence, this thesis report adds value by examining these two issues surrounding BC/DR. In this work, we attempt to respond to the following questions: w*hat is the current status of BC/DR practices? How have these been affected since the events of 9/11?*

This research project aims to fulfill two key objectives. First, this study will attempt to further increase contribution to the academic and practitioner communities by outlining several CSFs not referenced within previous research by utilizing exploratory analysis. Second, this project will examine whether the ranking of critical success factors (CSFs) for implementing a BC/DR program have changed from previous research, specifically subsequent to the events of September 11th, 2001 (9/11). In classifying factors, professionals and academics alike may gain a better understanding of what constitutes an effective BC/DR program and may likewise assist corporations in benchmarking how they rank relative to their industry.

The respondent in this report is the BC/DR practitioner. Such individuals are actively involved in some aspect of a corporate BC/DR program, whether coordinating, planning, analyzing, testing, implementing or maintaining this business function. Much BC/DR research and surveys have focused on the corporation ((KPMG & Continuity Insights, 2006; Chandler and Wallace, 2004; Envoy WorldWide, 2005b). However, views experienced by the practitioner can greatly contribute and expand the BC/DR field. These same individuals can influence top management commitment, and such commitment can garner the needed support to implement a BC/DR initiative from start to finish (Chow 2000; Botha and Von Solms, 2004) . Hence, the objective of selecting the BC/DR practitioner as the main unit of analysis is to determine how the effects of the September 11th, 2001 attacks (9/11) have impacted the practitioner's functions in an organizational setting.

Division of Thesis

We present this report as follows. In Chapter 2, we review the various definitions found in the literature with respect to the contingency planning field and identify those most relevant to this study. We next examine the concepts of BC/DR and present a brief history of the contingency planning field. Thereafter, we define the use of BC and DR, followed by the major benefits and inhibitors of each. In Chapter 3, we describe every CSF within Chow's study, reveal several emerging CSFs and complete the section with selected best practices to implement a BC/DR program.

In Chapter 4, we describe a multi-method approach used for data collection (the qualitative (interviews) and quantitative (survey) collection methods) by defining the methodology used. In Chapters 5 we describe and analyze collected results and consequently discuss these in Chapter 6, providing appropriate conclusions and discussion on propositions that were supported or unsupported as well as lessons learned. Chapter 7 describes the limitations of our work. Implications for both academics and practitioners are delineated in Chapter 8. and finally, Chapter 9 concludes by presenting avenues of potential research in the BC/DR field.

II. BACKGROUND

Interruptions Affect Us All...

The greatest misconception in BC/DR is the belief that an interruption will not adversely affect an organization in particular (Vijayaraman and Ramakrishna, 1993; Jacobs and Weiner, 1997; Sun, 2004). Nothing can be further from the truth: a study noted that 50% of those firms whose critical business systems go down for 10 days or more never recover, and 93% of the companies with no recovery plan fail within five years (Nelson, 2000; Anonymous, 2003c). Statistics prove that well-prepared corporations possessing an implemented contingency plan have been able to recover in a more effective and rapid manner (Carlson and Parker, 1998; Savage, 2002, Beck, 2004). Alarmingly, (as outlined in **APPENDIX I**) not many have taken heed of such advice.

As such, few corporations have taken a positive and pro-active stance on being able to deal with calamitous situations, creating undue stress and a sense of urgency to all those involved. A 2003 study of 300 business technology executives reported that 65% ranked BC planning and disaster preparedness as high priorities compared to 77% in 2002, a 12% decrease (D'Antoni, 2003). Consequently, the financial impact of a lack of preparedness has been demonstrated. **TABLE 1** below lists downtime costs within certain industries: corporations stand to lose hundreds, even millions of dollars of lost revenue per hour if disaster strikes.

FINANCIAL IMPACT BY INDUSTRY	LOST REVENUE / HOUR	LOST REVENUE / EMPLOYEE HOUR
Chemicals	$704,000	$194
Energy	$2,817,000	$589
Finance	$1,495,000	$1,079
Health Care	$636,000	$142
Information Technology	$1,344,000	$184

TABLE 1 Downtime Costs per Industry
(adapted from (Sun, 2004, p.4)

In a similar vein, studies indicate that such damage has repercussions on an array of stakeholders within the organization's spectrum (Laye and Torre-Enciso, 2001; Weiner, 2001; Botha and Von Solms, 2004). Business owners (in the private sector) and shareholders (in the public domain) receive less of a return on their investment and, more so, may lose their entire investment altogether. Employees may suffer a loss financially in terms of lost wages and may be emotionally affected by the disaster. The customer is impacted since the product provided may have been altered due to effects from the disaster. The consequent costs associated from recovery may have been passed on to him/her. Suppliers are affected since they may no longer provide goods/services to the organization until full recovery; and the government is at risk since it must do everything possible to aid corporations in recovering from the disaster, necessitating expenditure of funds and likewise decrease in earned revenues from taxes. Hence, reciprocal relationships between stakeholders and the organization can hold true solely if both sides continue to operate as normal. Any tear in the affiliation can have negative consequences (Paton, 1999).

Increased Dependence on Information Technology: the New Reality

For over 30 years, businesses of all sizes and all industries have steadily become increasingly dependent on their growing IT infrastructures to help them automate, manage and analyze their business operations and overall strategy. Chow (2000) indicates that IT and the design, implementation and management of enterprise information systems (ISs) are becoming a "basic infra-structural and operational necessity" (p.80). Corporations are recognizing the need to be at the cutting edge in the marketplace by constantly relying on efficient IT and IS methodologies, templates, tools, solutions, and services (Karakasidis, 1997; Carlson and Parker, 1998) and by having a competitive advantage over their competitors (Lee and Ross, 1995; Hawkins, Yen *et al.,* 2000; Sun, 2004. An example is the migration of the centralized, mainframe-based computer environment to the decentralized, LAN/WAN focused network environment (Hawkins, Yen *et al.,* 2000). If a server in the decentralized (or distributed), networked set-up fails, troubles arise for users and the corporation. Thus, reliance on external networks has spawned the need for more effective disaster prevention and mitigation (Cerullo and Cerullo, 2004).

No greater event revealed the increased reliance of IT than the Year 2000 (Y2K) crisis (Nelson, 2000). Millions of dollars spent by corporations worldwide ensuring that the transition would not cause ISs to crash resulted in no widespread disaster reported on January 1st, 2000 and the days thereafter. In a similar context, Banyopadhyay & Schkade's (2000) study of Health Management Information Systems (HMISs) revealed that Health Management Organizations (HMOs) adoption of DRP is positively related to the degree of reliance on HMISs. Such critical tasks as medical records, drug inventory and claims management are being increasingly computerized. Any disturbance in certain vital HMISs can cause harm to patients, a factor than no HMO would like to incur. Such dependency reflects the increasingly predominant change to the digital reality.

A. What is a Disaster?

Andrews (1990) simply states that a disaster is the "inability of an organization to function for whatever reason (p.29)". Concomitantly, the literature reveals that the corporation defines the extent of what constitutes a disaster; a specific event may be catastrophic to one organization but relatively mundane to the next (Green, 2003). Nonetheless, some common factors aid in determining what factors comprise a disaster. While in **APPENDIX II** we define all of the terms outlined in this paper, and some of the most relevant and cited categorizations of this concept, common examples of these factors are described below.

1. Natural Disasters

Natural disasters as earthquakes, tornadoes and floods, are unintentional, environmental forces that occur at any moment, affect multiple locations and are immune to human intervention. Many articles have outlined template contingency plans (Weiner, 2001) and helpful websites (Hane, 2001; Watson, 2004) assisting corporations to effectively respond to these types of well-documented disasters. Inasmuch, case studies have purported numerous lessons learned and emphasized the needed tools, policies and procedures in place to effectively recover from natural disasters (Arend, 1994; Dixon and Murphy, 1994; Purcell, 1994).

2. Human-induced Disasters

Human-induced (or otherwise termed man-made) disasters occur intentionally or unintentionally.

a) Unintentional Human Disasters

Examples include computer data loss (due to human error), mechanical failures, inadequate contingencies and logical security mismanagement. A recent example is the error in human judgment resulting in the hydro-electrical blackout of 2003 affecting several US Northeastern states (Ohio, Philadelphia, New York, Vermont amongst others) and a major part of the Canadian province of Ontario (Ballman, 2003; Phelan, 2003). The aftermaths of the August 2003 blackout made companies realize their lack of preparedness faced with a similar situation. However, many authors argue that repercussions can be effectively mitigated if proper measures are incorporated beforehand (Haight and Byers, 1991; Carlson and Parker, 1998; Castillo, 2004).

b) Intentional Human Disasters

Intentional man-made disasters are malicious in nature and may cause much harm. As reported in Karakasidis (1997), arson, bomb threats, riots and vandalism are several examples of this type of threat. However, no event of this kind has had the social impacts and repercussions as the attack on the World Trade Center towers on September 11th, 2001 (9/11). Several references (e.g.: (Mendoza, 2004)), case studies (e.g.: (Barr, 2003)), statistics and surveys (e.g.: (Anonymous, 2003c; Garvey, 2004), recommendations (e.g.: (Scarinci, 2002)) and reports (e.g.: (Scalet, 2001; Robinson, 2002)) have detailed the aftermaths of such an event. A common theme throughout these articles: threats have created the urgent need and fostered the awareness to prepare one's self in the event of another similar situation.

3. Technological Disasters

Similar to human-induced threats, technological disasters occur intentionally or unintentionally:

a) Intentional Technological Disasters

Those that occur intentionally are malevolent in nature and are intended to cause harm: computer viruses and worms, computer hacking and spamming are a subset of this vastly growing type of threat. A 2004 *Continuity Insights* survey estimated that American corporations lost approximately $10 billion in employee productivity from spam e-mails alone (Anonymous, 2004a). It is practically impossible to fully guard against the creation of such threats, but instilling such mitigating technologies as firewalls, intrusion detection systems, anti-spamming and anti-virus software may aid in combating this type of menace (Quirchmayr, 2004; Wilson, 2004; Hanna, 2005).

b) Unintentional Technological Disasters

Unintentional technological disasters usually occur as a chain-reaction from natural or human-induced disasters. For instance, an earthquake may have caused some wiring to short-circuit the server room, causing an electrical fire in the process. Such unintentional technological disasters are increasingly prevalent in organizations today (Iron Mountain, 2004). Nonetheless, these types of threats provide signals that uniformly register with all people involved, causing the appropriate measures to be in place (Chow, 2000).

As previously defined, technological disasters can occur as a chain-reaction from natural or human-induced catastrophes. It is incumbent that organizations establish the criteria defining a disaster since the proper response to a specific disaster may vary from one organization to the next. The level of tolerance and response time of the organization affect what constitutes a disaster.

As such, it is important to identify some common components or a single definition that guides the reader in understanding what constitutes a disaster. As mentioned in the outset of this chapter, **APPENDIX II** comprises a table with some of the most commonly cited definitions. For our purposes, we accept the Carlson & Parker (1998) definition of disaster as "any interruption in a company's overall operations that will significantly affect employees and/or customers. (p.11).

B. Comparing Disaster Recovery and Business Continuity

1. Ambiguity of Definitions

The DR and BC concepts are widely used in the literature and, in an erroneous fashion, have even been used interchangeably (Jacobs and Weiner, 1997). Elliott, Swartz *et al.* (1999) attest that there is no formally accepted definition of what constitutes either term. "Ask 20 different people for their concept of contingency planning and you will probably get 20 different answers." (Andrews, 1990, p.29).

This confusion arises from the fact that there is no single, widely agreed-upon definition outlined by some governing body (McCracken, 2005). Although such terms may mean different things to various organizations and authors alike, there are common items that are readily apparent in both concepts that need to be discerned.

2. Disaster Recovery: a Subset of Business Continuity

It is equally important to understand that disaster recovery (DR) is a subset of business continuity (BC) (Lethbridge, 2001; Hood, 2005). As such, BC implies DR but the reverse cannot likewise be stated. Recovering the entire business from a disaster implies recovering the IT function, but recovering a specific function as IT does not ensure that the business will also recover.

3. Business Continuity: Concepts

BC emerged mainly in response to the increased corporate realization that any disruption in the continuity of the business for an extended period of time seriously affected the overall viability of the company (Carlson and Parker, 1998). Simply recovering the IT function was not enough; the business needed to resume as quickly and as efficiently as possible (Moore, 1995; McCracken, 2005). Recovering the business function entails numerous corporate objectives as market share, cash flow, preservation of customer base, and corporate image, that need to be constantly met. These measurable goals are adversely affected the greater the time to recover from a disaster: as time progresses within a disaster and if nothing is being done, market share declines, cash flow decreases, customers switch and the company's reputation suffers. Hence, importance lies within the recovery and continuity of the entire corporate function, not just IT (Wong, Monaco *et al.*, 1994; Karakasidis, 1997; Chow, 2000). Such an approach can be justified as multi-disciplinarian (Beck, 2004), holistic (Elliott, Swartz *et al.*, 1999), and "proactive" (Hawkins, Yen *et al.*, 2000; Castillo, 2004).

Likewise, BC is the culmination of numerous other factors that have been reported in the literature. Globalization, increased competitive pressures, accountability from directors and officers, and strict government regulations are a subset of the reasons why BC has flourished into what it is today. This amplifies the need to ensure that business operations are not affected for an extended period of time (Alonso and Boucher 2001; Weiner, 2001; AT&T, 2004). The emphasis should no longer be on business recovery, but on business continuity (Heng, 1996).

Concepts of BC, the business continuity plan (BC Plan) and business continuity planning (BCP – or otherwise known as business continuity management (BCM) - (Msezane and McBride, 2002)) are respectively described and reviewed from the literature in **APPENDIX II.** For the purposes of this thesis, the following definitions of the latter concepts will hold throughout the report as they derive from the most respected and valued body of knowledge in the field of BC/DR: the *Disaster Recovery Journal* (except where noted).

Business Continuity (BC): The ability of an organization to ensure continuity of service and support for its customers and to maintain its viability before, after and during an event (DRJ, 2006).

Business Continuity Plan (BC Plan): The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals. (DRJ, 2006).

Business Continuity Planning (BCP): The documentation of the strategies, procedures, resources, organizational structure and information database utilized by an organization to respond to, recover from, resume and continue operations in the event of a substantial disruptive incident. (Msezane and McBride, 2002, p.349).

4. Disaster Recovery: Concepts

The field of DR started over 40 years ago in response to the emerging popularity of IT (Hawkins, Yen *et al.*, 2000). "Most organizations are so dependent on computer processing that they cannot operate without it" (Haight and Byers, 1991). As society transitioned from the industrial to the information age, reliance on information grew steadfastly. Consequently, corporations became more aware of their need to have a process in place to recover their competitive advantage (Chow, 2000; Hawkins, Yen *et al.,* 2000). Organizations acknowledge that a completely secured system cannot be devised and a completely full-proof DR Plan is impossible (Cerullo, 1981; Lethbridge, 2001). Such a "reactive" approach (Castillo, 2004) to recovery mitigates the many inherent risks should a disaster occur. Iyer & Bandyopadhyay (2000) reveal that by having a process in place as a fully functional recovery facility (hot site) or simply an area where an organization can recover its main IT assets (cold site), a recovery strategy can be devised and implemented. Whether documentation is as detailed as having the step-by-step instructions on how to recover any related IT-function or a brief document summarizing the tasks to be accomplished in response to a disaster, possessing and implementing a written plan is worth the cost and effort (Lethbridge, 2001).

As organizations grew more dependent upon IT systems, safeguarding such assets became a higher priority and more commonplace in many organizations (Savage, 2002; Mendoza, 2004). This increasing reliance through electronic means meant that something had to be implemented quickly if disaster were to strike. Where companies were almost at the mercy of their IT infrastructure, it became necessary to mitigate the impacts of such an occurrence. The end result was a "living, breathing, detailed document" (Hawkins, Yen *et al.*, 2000) used to mitigate the effects of a disaster's impact. The concept of a disaster recovery plan (DR Plan) was coined.

In summary, we have selected from **APPENDIX II** the following definitions to precisely encompass the essence of DR concepts since these reflect the most enduring and used referenced to DR: the *Disaster Recovery Journal.*

> Disaster Recovery (DR): Activities and programs designed to return the entity to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions (DRJ, 2006).
>
> Disaster Recovery Plan (DR Plan): The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals (DRJ, 2006).
>
> Disaster Recovery Planning (DRP): The technological aspect of business continuity planning. The advance planning and preparations that are necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster (DRJ, 2006).

5. Business Continuity & Disaster Recovery Compared

Although many similarities exist between DR and BC, differences between them do arise. **TABLE 2** illustrates the main differences found in the literature.

CHARACTERISTIC	**DRP**	**BCP**
PRACTICE	Standard	Better
VISION	Old	New
FOCUS	IT	Business
STAFF	IT	Multi-Disciplinary
STRUCTURE	Existing	New
AIM	Protect Core Operations	Protect Organization
EMPHASIS	Recovery	Prevention
RECOVERY APPROACH	Single-Focus	Holistic
REACTION	Reactive	Proactive

TABLE 2 Disaster Recovery and Business Continuity Planning Compared (adapted from *Figure 1*, Disaster Recovery and BCP Approaches Compared, Elliott, Swartz *et al.*, 1999, p.49)

As summarized above, internal and hardware-focused DR strategies are labeled as "standard" practice (Elliott, Swartz *et al.*, 1999) since the latter's focus is IT driven, i.e., as long as systems and infrastructure work, the recovery effort is deemed a success. Contrary to this practice is the more holistic recovery approach of the "better" practice organization (Elliott, Swartz *et al.*, 1999), p.45). Customers, suppliers, employees and vendors are considered part of this practice in an emergency situation since such strategies treat IS security issues within a "greater internal-external, hardware-software framework". Another important criteria are the embedded recovery procedures, policies and structures of "better" practice organizations. Emphasis is on prevention, not solely on recovery. While such procedures, policies and structures are being established, activity and involvement of all business functions are being elicited. Proactive, multi-disciplinary staff involvement differs with regards to the old vision of recovery where IT is the sole proprietor of the recovery function.

C. History of Business Continuity / Disaster Recovery Field

Despite the existence of natural disasters since the beginning of time, the field of recovery planning is relatively new in contrast to such areas as psychology, sociology and other social sciences (McCracken, 2005). Throughout this thesis report, numerous disasters within the last 20 years are mentioned, with an added emphasis on the Year 2000 (Y2K) and September 11th, 2001 (9/11) crisises. In this section, we present an overview of 4 issues in the history of BC/DR.

1. Disaster Recovery, Business Continuity and the Information Technology Evolution

Coined in the early 1960's, disaster recovery (DR) was used solely by larger-scale organizations spanning multiple locations. In essence, data typically resided on stand-alone IBM mainframes (Andrews, 1990; Rosenthal and Sheiniuk, 1993; Heikkinen and Sarkis, 1996). Paradine (1995) contests that during this era, the DR Plan was similar to an insurance policy that simply offered protection from natural disasters. In the 1970's, the "technological" mindset (Pitt and Goyal, 2004) meant that the focus was on the protection of computer-based systems residing on corporate, robust mainframe systems as opposed to less manageable PCs (Chow, 2000). Consequently, mission-critical data was being stored throughout entire enterprise networks and safeguarding such assets became crucial. Hawkins, Yen *et al.* (2000) explain that as distributed systems and globalization started to emerge, the need to have an effective plan to recover the entire business started to gain widespread acceptance.

Accordingly, the concepts of client/server architecture and business continuity arose in the 1980's and protecting data and systems across national boundaries became a major corporate priority. The latter changes brought about the "auditing" mindset of the 80's (Pitt and Goyal, 2004). As explained in Chow (2000), such "local/wide area network"-based systems (LANs/WANs) replaced those in the mainframe environment. The drive to the 1990's was brought about by the explosion of the Internet and the consequent "value" mindset of organizations (Pitt and Goyal, 2004). Being focused on the needs of the business and having BC add potential value to the company was starting to flourish (Lethbridge, 2001). In response, establishing a proper recovery strategy became paramount on corporate agendas. With the increased threats of man-made disasters, especially the technological kind (e.g.: worms, viruses, Trojans, spam, phishing, hacking...), surviving did not mean recovering the technological function: it meant recovering the whole business as rapidly and efficiently as possible.

Hence, the field of BC planning evolved from simple "reactive" DR planning (technology mindset), to crisis management principally driven by IT (auditing mindset), and finally to the "proactive", comprehensive and holistic approach (value mindset) used today (Bandyopadhyay and Schkade, 2000; Pitt and Goyal, 2004). Taking the value mindset described previously, the transition to the new millennium was characterized by a couple of events that re-shaped the way corporations think, react and treat BC/DR, i.e., Y2K and 9/11.

2. The Year 2000 (Y2K) Crisis

The Y2K crisis triggered much needed awareness of DR and BC at the corporate level (Hensley and Zane, 1998; Nelson, 2000). Upper management realized the magnitude of repercussions that could stem if they were not prepared in time to rollover to January 1st, 2000. As well, regulators - especially in the financial sector - needed to ensure that companies across the country were well prepared in the event of any possible threat stemming from the Y2K rollover (Hensley and Zane, 1998; Bielski and Cocheo, 1999; Marlin, 1999). As Riley (1999) reported, millions of lines of code needed to be re-programmed in order to ensure that all systems, from payroll to nuclear reactors, were compliant with the transition to the Year 2000.

In turn, corporations developed basic risk analysis techniques from critical impact assessments of the various applications and systems. This aided practitioners in eventually developing and implementing contingency plans (Mendoza, 2004). Issues such as liquidity of money in Automated Teller Machines (ATMs) within the banking industry were of primary concern. As such, contingency plans were one of the main means to mitigate the likely effects of Y2K (Riley, 1999).

3. The September 11th, 2001 Attacks

No other disaster, whether natural or man-made, has had the repercussions and likely effects on society as the events of September 11th, 2001. In no time in history has a single disaster conjured up the awareness, revealed the degree of vulnerability and promoted needed education in terms of reports, surveys, stories, case studies and lessons learned to sensitize the population on the importance of BC and DR (Bielski 2003; Castillo 2004; Iron Mountain, 2004).

New trends within the BC/DR fields started to emerge in the post-9/11 era and increased focus was occurring regarding effective and rapid communication. Products and services such as *EnvoyWorldWide*'s Enterprise Notification Services® (Envoy ENS, 2006) and *MessageOne*'s AlertFind Enterprise® (MessageOne, 2006) are a subset of the recent technological advances gaining increased presence due to the events of 9/11. As such, corporations have emphasized the significance of having BC/DR instilled into their culture in order to strive and survive (Savage, 2002; Pitt and Goyal, 2004; Sun, 2004). Pre-9/11, data and information was of prime importance if disaster struck and having data replicated and backed up was of great importance. Since the attacks, success of any contingency plan depends upon the people (Iyer and Bandyopadhyay, 2000).

4. Legal & Regulatory Requirements

As part of the global business process to appease shareholder and consumer confidence (Grillo, 2003), legal and regulatory requirements have been mandated upon organizations of all sizes pursuant to the events of 9/11 to implement effective internal controls and possess well-documented procedures and policies with regards to public reporting (Weiner, 2001; Beck, 2004; Sun, 2004). Corporations serving the public interest such as financial institutions, airports and blood banks are more likely to have contingency plans in place due to legal, financial and statutory requirements (Luecke and Hoopingarner, 1993; Wong, Monaco *et al.*, 1994, Grillo, 2003). Customers, clients, shareholders and the government need to be reassured that their corporate interests are being proactive when faced with any type of disaster. Some of the most important and recent laws since September 11th, 2001 are explained below.

- Concerning BC/DR regulations, the financial industry (representing most notably banks, trusts and mortgage companies) is one of the greatest proponents of instituting an effective recovery program (Luecke and Hoopingarner, 1993; Dow, 2004). The Financial

Services Act (FSA) of 1986 in the UK and the more stringent 1983 US Banking Circular 137 are examples of financially imposed legislation. All US financial institutions must be able to conduct "business as normal" within 24 hours following a disaster by developing means to reduce the impact and/or risk of losing data processing support (Wong, Monaco *et al.*, 1994, Lee and Ross, 1995; Bandyopadhyay and Schkade, 2000), including such provisions as backup data centers and offsite tape storage (Dow, 2004).

- No other corporate regulatory act has had the impact on business and the issue of contingency planning stemming from the events of 9/11 as the Sarbanes-Oxley Act of 2002 (SOX). Section 404 requires that executive accountability measures be in place to validate internal controls, that corporations remain responsible for controls of any outsourced activity, and that these institutions regularly report to shareholders on their viability (Chalaka, 2003; Berman, 2005). Klein (2005) iterates that external auditing must assess the completeness, accuracy and timeliness of control activities and processes, be involved in these risks and ensure effectiveness by conducting periodic testing. Tools such as archiving systems are being implemented as a way to ensure compliance to SOX (Archivas, 2004; Kenniston, 2005). Gibson (2005) asserts that even though many corporative executives view costs associated to SOX as exorbitant, they are finding out that becoming compliant has made their organization(s) more efficient and effective. Supporting this claim, 88% of CIOs say that their IT departments are very involved in compliance to the SOX Act (Perez, 2005). Failure to act and become compliant by July 2006 may result in hefty financial penalties to corporations and even jail time to executives found guilty (Klein, 2005).

- The Health Insurance Portability and Accountability Act (HIPAA), enacted to ensure that private health information remains as such, no matter the communication method used, was designed to protect and enhance the rights and integrity of consumers by improving access to their personal health information (PHI) and to provide control over patient information uses and disclosures (Chalaka, 2003; Pumo, 2004; Cardona, 2003). Covered entities – including healthcare providers, healthcare clearinghouses, health plans and other healthcare institutions – must comply within 24 months of the effective date of this regulation or else face criminal and civil penalties (Cardona, 2003). Policies and procedures need to be implemented as of April 21st, 2005 ensuring US healthcare organizations protect the availability, integrity and security of information during unexpected, negative events (Padilla, 2005; Cardona, 2003). Implementing a sound and effective contingency program according to standards within the Privacy Rule (see (Pumo, 2004)) will provide efficient safeguards and controls for the protected health information of any organization (Cardona, 2003). Following the common contingency implementation steps will help in accomplishing such results.

- Similar in concept to HIPAA, the Gramm-Leach-Bliley (GLB) Act prohibits financial institutions from sharing a customer's "nonpublic financial information" with non-affiliated 3rd parties. Enacted on November 12th, 1999 and geared to financial entities, the Privacy Law stipulates protecting the confidentiality and integrity of personal consumer information as its prime objective. Compliance for federally regulated entities was required by July 1st, 2001 (Archivas, 2004).

In sum, protecting consumer information from exposure in the event of a disaster and ensuring visibility and accountability of one's actions, whether in the financial, healthcare or other industry, are the ultimate goals of US legislation since the events of 9/11. Even though many companies are lagging behind in compliance (Klein, 2005; Berman, 2005), these acts are passed into law to protect the end consumer. **APPENDIX III** summarizes the most prominent financial US regulations since 9/11 (Archivas, 2004).

D. Business Continuity and Disaster Recovery in Organizations

Understanding the importance of organizational BC and DR and the main benefits and drawbacks of such an approach issues are crucial in the context of this study.

1. Importance of Business Continuity / Disaster Recovery

With the growing dependence of IT in organizations and the proliferation of distributed computing worldwide, it has become evident that the need to effectively recover from a disaster is gaining increasing importance. Several studies crystallize the relative importance of BC and DR on today's corporate agenda (Garvey, 2004; Sun, 2004). In essence, the impetus of BC/DR in organizations has pragmatically shifted from "nice to have" to "should have" to "must have" in some industries (Savage, 2002). Laye & Torre-Enciso (2001) explain that this movement stems primarily from the events of 9/11 and recently imposed regulations from the fear of having unnecessarily prolonged disruptions. Statistics show that the average length of an outage for companies with a contingency program in place is 6 hours compared to 10 hours for those corporations without a program in place (Rodriguez, 1997). Each hour of outage can equate to millions of dollars in losses (see **TABLE 1)**

In a similar vein, the contingency planning industry has likewise witnessed the gradual evolution from IT DR to business continuity planning (BC) to the most recent, supply-chain focused business resumption planning (BR), the latter covering all stakeholders in case of a disaster. As stated by Moore (1995), "a well designed, implemented and tested contingency plan is the best measure against financial peril for any organization, institution or organization with a future (p.22)". Companies must fully embrace an integrated and holistic approach to BC within their corporate objectives to ensure a full and successful recovery from catastrophe (Msezane and McBride, 2002).

Carlson & Parker's (1998) study of 400 US Certified Management Accountants (CMAs) indicated that over 90% of institutions are dependent on computer systems. Millions of dollars are at stake if proper measures and factors are not in place prior to a disaster occurring. No greater proof can reflect the importance of having a contingency plan implemented than publicly reporting possible financial losses that may stem from prolonged disaster. A study of manufacturing and distribution companies with yearly gross sales of over $215 million revealed that a "typical company will lose over $100,000 after four days without IS services and over $1 million after 10 days." (Wong, Monaco *et al.*, 1994, p.29). The same study revealed that the average corporation will "lose over 12% of its gross annual sales within eight days of sustained outage". In addition, companies that were heavily dependent on IT tended to be furthest along the BCP path (AT&T, 2004). It is therefore apparent that corporations not only have to prepare themselves, but also have to ensure that entities within their supply chain are also well prepared in the event of a disaster (Elliott, Swartz *et al.*, 1999; AT&T, 2004).

2. Major Benefits of Business Continuity / Disaster Recovery

All stakeholders benefit from having a well-implemented and properly documented BC/DR program. Internally, confusion regarding recovery duties, corporate disruptions and reliance on key individuals decrease and the safety of employees is consequently provisioned for. Externally, benefits include increased corporate credibility. As such, implementing an effective BC/DR program in any organization results in numerous benefits, as defined below.

a) Elimination of possible confusion and error

Customer relations, employee morale, company image, vendor dealings and legal issues need to be addressed when disaster strikes. Having assigned specific duties to response teams, management can focus their efforts to critical contingency issues, thus alleviating much confusion as to assigned responsibilities. (Paradine, 1995; Jacobs and Weiner, 1997; Iyer and Bandyopadhyay, 2000).

b) Reducing disruptions to corporate operations

A properly implemented BC/DR plan will define the selected alternate recovery site within the first few hours of a disaster occurring. As such, recovery time is greatly reduced since preparations with respect to recovery of systems and services have been accounted for (Hawkins, Yen *et al.*, 2000; Iyer and Bandyopadhyay, 2000).

c) Documented alternatives during a catastrophe

A well-designed and documented BC/DR plan allows top management to take the time to judicially consider all alternatives when selecting the best choice for proper recovery, lessening the amount of time to decide upon the wisest choice in the event of a disaster. (Paradine, 1995; Hawkins, Yen *et al.,* 2000; Iyer and Bandyopadhyay, 2000).

d) Reducing reliance on key individuals

Having properly documented and developed contingency plans coupled with well trained personnel lessens the risk of relying upon a few key individuals to perform particular functions during the recovery process. As such, any resource can follow what is written to effectively recover (Hawkins, Yen *et al.*, 2000; Iyer and Bandyopadhyay, 2000).

e) Proper data protection

Touted as the most vital non-human component of an organization, data needs to be properly stored to effectively recover this corporate asset in the event a disaster. Storage media as tapes and hard disks and storage formats as databases, spreadsheets and documents need to be properly protected from catastrophe (Hawkins, Yen *et al.*, 2000).

f) Employee safety

Touted as one of the main objectives of any well-developed contingency program, implementing safeguards to provide for the well-being of employees – the lifeblood of any corporation - is the essence of creating a BC/DR plan (Hawkins, Yen *et al.*, 2000).

g) Having an orderly recovery

Another sought-after benefit of possessing a well documented BC/DR procedures is having a procedural approach to recover from a disaster. Numerous studies have shown that corporations having a properly documented, implemented, tested and maintained plan recover more effectively than those not possessing one (Karakasidis, 1997).

h) Increased credibility and value-added to the organization

By having documented contingency procedures, the organization's value is increased as is its credibility to the eyes of potential buyers, shareholders and the general public. Individuals are more likely to invest in a company that has sound, effective and tested contingency plans that a corporation that does not (Jacobs and Weiner 1997).

3. Major Inhibitors of Business Continuity /Disaster Recovery

Although DR and BC allow firms to effectively recover from a disaster, major inhibitors to such strategies do exist and include such factors as properly justifying costs regarding a BC/DR program, corporate barriers including a lack of management support and resources, and a lack of common terminology and relevant research. These and other major inhibitors are explained below.

a) Cost & ROI

Increasing exponentially over time, one of the most cited inhibitors in the literature is the issue of financial cost (Hawkins, Yen *et al.*, 2000; Nahum, 2003, Pisselo, 2002). A 2003 study noted that worldwide IT spending reached $64 billion in 2002 and is projected to surpass $118 billion by the end of 2007 (Sun, 2004, p.21). Not only do direct, tangible costs of implementation (e.g.: software, hardware, telecommunications and salaries) hinder the decision to adopt a BC/DR initiative, but indirect, intangible costs (e.g.: loss in consumer confidence, damaged reputation and loss of competitive edge) are an increasing corporate preoccupation (Rohde and Haskett, 1990; Vijayaraman and Ramakrishna, 1993; Lee and Ross, 1995).

It is commonly revealed that a positive ROI is crucial to a point that upper management executives will not further support a BC/DR initiative in a post-planning stage if it is not positive. A 2004 survey of IT executives indicated that more than 90% of all projects now require a positive ROI justification (Pisselo, 2002). Consequently, a decision to no longer pursue implementation of a BC/DR program stems from the belief that return on investment (ROI) is not readily quantifiable and justified (Lee and Ross, 1995; Buffington, 2002, Buffington, 2003; Faile and Mucisko, 2005). It is critical to present a credible business case that clearly defines the measures and benefits of a BC or DR plan (Beck, 2004). Corporations relying on this financial indictor are omitting important non-financial information as "elusive" intangible costs are imperative to take into consideration when justifying investment in BC/DR. Conversely, accurately quantifying the latter is almost impossible, creating a paradoxical issue and managerial challenge. Thus, ROI – and more importantly cost – is an important factor but should not be considered the sole, deciding factor.

b) Lack of Management Support

Initiatives have a greater chance of failure than success if lack of management support to adopt and implement a BC/DR program is apparent (Jacobs and Weiner, 1997; Buffington, 2005; Oh 2005). Carlson & Parker (1998) found that 33% of their respondents agree that lack of executive buy-in was the main reason why their corporation did not have an effective DR plan in place. To mitigate the latter, responsible resources should educate all levels of management staff (lower, middle and upper) on the importance of instilling a BC/DR program from the initial phases of implementation (Cale and Dye, 1998; Carlson and Parker, 1998). In fact, several authors assert that this should be part of corporate culture (Savage, 2002; Pitt and Goyal, 2004).

c) Low Priority

To be deemed successful, any corporate executive member wishing to institute a BC/DR program must think of the latter as a high priority prior to implementation. Studies have revealed that there is a positive correlation between the level of priority of BC or DR within the organization and implementation success: the greater the level of priority within the boardroom, the greater the rate of success from consequent implementation (Cale and Dye, 1998; Carlson and Parker, 1998). As such, it is crucial that BC/DR be communicated as an important priority throughout the organization for successful implementation (Jordan, 1999; Oh, 2005). Only through proper awareness and training – at all levels in the company – can BC and DR gain much needed importance and become a top priority.

d) Lack of Common Terminology

Contingency planning notions as defined in **APPENDIX II** abound with multiple definitions of similar concepts found in this field (Andrews, 1990; Buffington, 2005; McCracken, 2005). As such, confusion is often the result from this lack of common terminology (Bielski, 2003) since the origins of the discipline may explain the causes of this latter (McCracken, 2005). Some say this lack of consensus has lessened the credibility of the contingency planning spectrum and created a need for academics to establish a set of universal definitions (Andrews, 1990; Elliott, Swartz *et al.*, 1999; Green, 2003; Pumo, 2004; McCracken, 2005). In response to the latter, well-established and recognized associations as DRI (*Disaster Recovery Institute*) and DRIE (*Disaster Recovery Information Exchange*), and journals as DRJ (*Disaster Recovery Journal*) and *Continuity Insights* need to call upon academics to provide common definitions for each concept. This would strengthen the validity and credibility behind the theory and might further develop as an area of future research within the IT realm. Hence, BC professionals need to use consistent terminology and non-convoluted terms to avoid confusing people (McCracken, 2005).

e) Lack of Research

A consequence from the lack of common terminology is the lack of research (Rohde and Haskett, 1990; Nelson, 2000). Many authors infer that contingency planning proponents have not done enough to further the understanding and consensus of proposed terminologies and best practices in the field leading to better and more thorough research (Vijayaraman and Ramakrishna, 1993; Heikkinen and Sarkis, 1996; Botha and Von Solms, 2004). As such, absence of integration and agreement amongst industry practitioners and academics may be the reason why more research is needed. A perfect example of the lack of research in the BC/DR field is the search results of such academic databases as ProQuest® as summarized in **APPENDIX IV** that produce a very small subset of academic related material within the BC/DR field. **APPENDIX V** illustrates sample query screenshot and the generated results.

f) Increased Regulations

Throughout the years, there has been increased government scrutiny on corporations of all sizes to ensure that institutions safeguard consumer information, implement proper internal controls, and ensure accurate financial reporting. Mentioned previously, recent legislation as the Sarbanes-Oxley (SOX) Act, the Health Insurance Portability and Accountability (HIPAA) Act and the Gramm-Leach-Bliley (GLB) Act are several examples of safeguards passed and enacted to ensure that processes, policies and procedures are effective, well-documented, tested and audited (Johnson, 2005; Padilla, 2005).

g) Lack of Resources

Ensuring that sufficient resources – knowledgeable and trained on the contents of the program – are available and willing to participate in disaster recovery may impede a smooth transition to recovery (Rohde and Haskett, 1990). A dominant reason given in a study conducted by Jordan (1999) about the omission of a contingency plan (whether BC or DR) is insufficient resources. Five organizations from the participating 27 (or 18.5%)

confirmed that a lack of staff was the principal reason for not implementing a BC plan. To reiterate the citation from Iyer & Bandyopadhyay (2000) "the success of any BC/DR plan depends upon the people" (p.259).

In sum, disasters have been and will always be a part of life. Understanding the types of disasters, the impacts on diverse stakeholders and the mitigating BC/DR strategies used to counter the effects of a disaster, organizations can better prepare themselves in the event of a catastrophe. By understanding the importance of BC/DR, associated concepts, strengths and obstacles, an efficient BC/DR Plan can be created. Attaining this efficiency will be described in the following section, as the main critical success factors (CSFs) in effectively implementing a BC/DR program will be described.

III. CRITICAL SUCCESS FACTORS (CSFs)

One of the objectives of this study is to determine if the critical success factors (CSFs), as defined in the context of a BC/DR implementation program and referenced within Chow's (2000) study, have changed since the events of 9/11. Since the author's study was conducted prior to Y2K and 9/11 incidents, these were not an issue at the time of his study. Hence, this thesis report adds value by examining these two major issues surrounding BC/DR.

This section defines the concept of CSFs, outlines the top ones found in the literature and proposes a matrix classification of the top CSFs. Throughout the study, hypotheses are stated, culminating in the main research questions asked.

A. Defining Critical Success Factors

Different streams within the social sciences define CSFs in various ways. Several interpretations are delineated in **APPENDIX II**. For this study, the following definition is accepted:

> CSFs are a few performance measures which, if they are achieved satisfactorally, will ensure successful competitive performance for the organization. They are the

things that must go right and therefore, critical attention must be paid to these success factors. (Rockart, 1979).

CSFs exist in every organization and evolve throughout the organization's history. They tend to follow the "SMART" concept, i.e. they should be Specific, Measurable, Attainable, Realistic and Time-based. However, they must go beyond the traditional project measures of on time, on budget and to specifications since CSFs are measures of project performance and not project management. (Rockart, 1979).

1. Main Cricital Success Factors Defined

Using Chow's (2000) study of 400 companies from the banking, hotel, trading and manufacturing industries, this section examines the CSFs in light of the latest evidence and empirical research. As such, **APPENDIX VI** presents a classification and cross-referencing of the literature, summarizing the most important and readily cited CSFs.

CSF 1: Top Management Commitment

Numerous authors state that it is imperative that a contingency program be initiated, supported, approved and authorized by upper management as of the initial stages of implementation (Arend, 1994; Chow, 2000; Hawkins, Yen *et al.*, 2000). Top management is the sole corporate entity that can provide and secure large amounts of resources, capital and time (Chow, 2000; Botha and Von Solms, 2004) within such BC/DR life cycle activities as planning, analysis, testing, and maintenance (Wong, Monaco *et al.*, 1994; Bandyopadhyay and Schkade, 2000; Cerullo and Cerullo, 2004) - see **APPENDIX VI** for additional references. Hence, upper management must thoroughly understand, approve and authorize all BC/DR related activities before giving their final consent (Rosenthal and Sheiniuk, 1993; Sun, 2004).

Supporting this assertion, authors emphasize such adjectives as "most critical", "vital", "imperative", "paramount" and "essential" when discussing this CSF, as evidenced by several passages contained in **APPENDIX VII**. Furthermore, this factor was the most cited and recognized of the 18 described in Chow's study. **APPENDIX VIII** outlines how management views BCP in light of the events stemming from 9/11. As such, corporations are unprepared despite events of 9/11 (Anonymous, 2004c). A lack of top management support ultimately results in recovery failures, poor implementations and lack of personnel involvement (Cale and Dye, 1998; Nelson, 2000; Payne, 1999).

In a similar vein, a lack of top management understanding also impedes the effective implementation of a BC/DR program (Pitt and Goyal, 2004). Properly training and educating executive personnel by ensuring an understanding of BC/DR planning terminology and definitions is essential during the initial stages of a contingency program (Iyer and Bandyopadhyay, 2000). Properly understood, executive management can then effectively review the plan with all involved to ultimately gain approval (Luecke and Hoopingarner,1993; Lim, 2003). Several studies recommend that a member (or members) of top management be part of the designated BC/DR committee since such implication greatly increases the chances that upper management is committed to the project and that all necessary funds and resources are allocated and accounted for (Cerullo, 1981; Elliott, Swartz *et al.,* 1999).

As such, this factor is the first of 10 key elements from *DRII's/BCI's* Common Body of Knowledge (**APPENDIX IX**). Top management support is obtained within the Project Initiation and Management phases. Hence, being a top rated CSF within Chow's (2000) study and *DRII's/BCI'*s Common Body of Knowledge, it is logical that this CSF will remain as important as it was in past research.

CSF 2: *Adequate Financial Support*

Initial stages of implementing a BC/DR program cannot commence without proper financial support by executive management (Karakasidis, 1997; Grillo, 2003; Cerullo and Cerullo, 2004). In one survey, thirty-eight percent (38%) of BC/DR practitioners confirmed that the biggest challenge in planning contingency efforts was funding (Surmacz, 2001). Deemed "one of the greatest barriers to launching a successful DRP" by Chow (2000), financial support must be sufficient from the outset to ensure that all direct and indirect costs are weighed against the perceived benefits (Bandyopadhyay and Schkade, 2000).

CSF 3: Alignment of Disaster Recovery Planning Objectives with Company Goals

A BC/DR program should be driven by business needs to consequently create a competitive advantage in the form of more resilient systems (Elliott, Swartz *et al.*, 1999). Management will be increasingly committed if they perceive that organizational goals are aligned with BCP/DRP objectives (Wong, Monaco *et al.*, 1994).

Accordingly, strategies developed to ensure proper alignment of BC/DR objectives to corporate goals include creating checklists, conducting business impact analyses (BIAs) and properly completing disaster post-mortem reports (Lee and Ross, 1995; Paton, 1999; Beck, 2004). In order to ensure consistency within the corporation, proper analysis can be conducted at this stage since pre-determined BCP/DRP objectives are validated and amended accordingly (Grillo, 2003).

CSF 4: Adoption of Project Management Techniques

Project management (PM) techniques such as task management, resource allocation, scheduling and budgeting constitute the foundation of proper planning, development and implementation of any project (Heng, 1996; Karakasidis, 1997; Chow, 2000). Ensuring that all resources (monetary, time and human) are properly managed throughout a BC/DR project translates into positive returns. Examples include decreased reliance on certain key individuals (Hawkins, Yen *et al.*, 2000), establishing a project methodology and framework (Beck, 2004; Quirchmayr, 2004), and effectively communicating the project's deliverables (Jacobs and Weiner, 1997).

CSF 5: Presence of a Formal Recovery Planning Committee

Assembled and appointed by top management, a formal recovery planning committee must be created to ensure proper integration and coordination amongst team members (Rohde and Haskett, 1990; Luecke and Hoopingarner, 1993; Karakasidis, 1997). Functions include performing risk analysis for each area of the organization (Hawkins, Yen *et al.*, 2000), assigning key tasks to individuals (Jacobs and Weiner, 1997), supervising the recovery effort (Cerullo, 1981), and defining the scope, objectives and key success factors of the recovery process (Karakasidis, 1997). Focus should be to validate that responsibility of the

BC/DR procedures is instilled in the day-to-day activities of all involved (Karakasidis, 1997), ensuring that each member has confidence in one another and that all involved have a proper understanding of each member's strengths and limitations in response to a disaster (Payne, 1999).

***CSF 6**: Participation of Representatives from each Department*

Many authors explain how properly executed recovery efforts cannot be implemented without representatives from each department (Haight and Byers, 1991; Msezane and McBride, 2002; Sun, 2004) – **APPENDIX VI** lists other contributions). Organizational representatives with similar functions must unite to form specific recovery teams. Examples include a restoration team, a crisis management team, and a logistical support team (Rosenthal and Sheiniuk, 1993; Hawkins, Yen *et al.,* 2000; Sugano, 2005). A particular team would ensure that all aspects of its recovery task(s) are well executed since such resources have a greater understanding of their respective business functions (Elliott, Swartz *et al.,* 1999; Clifton, 2000; Bielski, 2003). Hawkins, Yen *et al.* (2000) contend that this would allow management to focus efforts on other critical issues related to disaster recovery (e.g.: customer relations, company liability, legal issues, etc.).

Hence, effective and efficient recovery includes assisting, coordinating and assigning specific recovery tasks mandated by upper management within an identified recovery team (Savage, 2002; Beck, 2004; Oh, 2005). As Iyer & Bandyopadhyay (2000) state, "After all, people are the number one asset in any organization and the success of any DR/BC plan depends on people. (p.259)" Availability of staff is crucial upon ensuring that representatives from each department are involved in a contingency program (Payne, 1999; Paton, 1999). No operation, enterprise, service nor function affected by the events we are contemplating can continue without people. (Laye and Torre-Enciso, 2001). Such an assertion underscores the importance of having effective human resources aiding the recovery effort.

***CSF** 7: Engagement of External Consultant*

Outsourcing the recovery function to specialized recovery firms had gained popularity in the 1980's and early 1990's due to cost and labour considerations, most notably missing internal expertise and relevant BC/DR experience (Wong, Monaco *et al.* 1994; Jacobs and Weiner, 1997; Nelson, 2000). Benefits of employing external advisors include no internal bias, a specific level of expertise and the most up-to-date knowledge within the field (AT&T, 2004). However, a recent study conducted by Pitt & Goyal (2004) reported that approximately two-thirds of their sample population created recovery plans internally, with only 10% exclusively outsourcing the entire function. Whatever the corporation decides upon, consultants must effectively communicate the benefits of the BC/DR program to corporate managers and key personnel alike (Bandyopadhyay and Schkade, 2000).

In essence, an organization may call on the services of an external consultant to solely develop the procedures of the plan and the consequent implementation and testing of the latter, to aid internal staff throughout the implementation phase of the program (from planning to testing), or to completely review what has been currently implemented and detect any areas of improvements that internal staff had not noticed. (Moore, 1995; Chow, 2000; Quirchmayr, 2004). As Luecke & Hoopingarner (1993) summarize, if the appropriate resources do not exist in house, a corporation should seek and secure outside resources to complete the task. It is essential to avail the organization with the necessary talents to put in place the documentation that may well prove to be the very lifeblood of the institution in the event of a disaster.

CSF 8: Risk Assessment

An often referred to CSF, risk assessment must be conducted within the first phases of the implementation cycle to systematically assess the potential impacts of all unexpected events to the organization (Rosenthal and Sheiniuk, 1993; Wong, Monaco *et al.*, 1994; Smith, 1995). **APPENDIX VI** lists other articles referring to this CSF. Since corporate contingency plans are specific and tailor-made, all possible threats – whether natural or man-made, intentional or non-intentional – are of prime importance to further conduct an effective analysis (Clifton, 2000; Carvajal-Vion and Garcia-Menendez, 2003; Bielski, 2003). The ultimate objective of the risk assessment phase is to provide management with the necessary information to further evaluate – or analyze – each identified threat (Pitt and Goyal, 2004).

While assessing risks, it is important to consider all critical elements affecting an organization. Such factors as determining critical ISs, establishing recovery priorities and identifying target recovery times for each application need to be taken into account (Hawkins, Yen *et al.*, 2000; Savage, 2002; Castillo, 2004). Information is gathered principally through interviews and/or surveys with the resource(s) most implicated with the concerned application(s)/system(s). Results include detailed cost/benefit breakdowns (Paton, 1999), desired recovery time objectives (Laye and Torre-Enciso, 2001), classification schemes of application/system criticality (Cerullo and Cerullo, 2004) and established frameworks of risks (Iyer and Bandyopadhyay, 2000). Beck (2004) explains risk assessment as a component of a larger risk management program that justifies investment in BC/DR. By identifying specific threats to business operations and measuring each one's probability of occurrence, specific methodologies can be applied to justify the budget to find avoidance controls.

As the second key element of *DRII's/BCI's* Common Body of Knowledge termed "Risk Evaluation & Control" (see **APPENDIX IX),** the BC/DR Coordinator must determine the surrounding events that can result in disasters, the extent of such events and the mitigating factors needed to minimize loss.

CSF 9: Impact Analysis

Impact analysis evaluates all feasible risks to determine the vulnerability of each threat to the organization. Numerous articles describe the analysis that is applied for accommodating a single department, a business unit, or an entire company (Lee and Ross, 1995; Grillo, 2003; Oh, 2005) –**APPENDIX VI** lists other articles referring to this CSF). Findings from the analysis are properly classified and consolidated within an action plan, reviewed by personnel whose responsibilities include analysis, and approved by upper management. (Karakasidis, 1997; Hawkins, Yen *et al.*, 2000; Green, 2003). The action plan can then be integrated to the corporation's business strategies and employees effectively trained to respond to each threat if something were to occur (Haight and Byers, 1991; Hawkins, Yen *et al.*, 2000).

Interviews and/or surveys would allow for cost/benefit analysis, criticality classification schemes, and impact frameworks within this stage (Wong, Monaco *et al.*, 1994; Cerullo and Cerullo, 2004; IronMountain 2004). A sample criticality classification would be to identify key business processes and examine the effects of disaster scenarios on each item using pre-defined time bands – e.g.: less than 2 hours; 2 to 24 hours; 1 to 5 days; greater than 5 days (Savage 2002; Bielski 2003). These results would allow management to link defined risk impacts to corporate objectives and ultimately come up with the appropriate recovery strategy.

Identifying organizational impacts and the techniques to quantify and qualify them comprise the third element of *DRII's/BCI's* Common Body of Knowledge (**APPENDIX VI**). **APPENDIX II** outlines the main definitions of impact analysis referenced in the literature.

CSF 10: Determination of Maximum Allowable Downtime

Surveys have shown that fewer than one in three North American companies believe that their contingency plan would meet their pre-defined recovery objectives if a disaster occurred (Sun, 2004). Determining maximum allowable downtime of critical information systems (ISs) portrays a clearer picture of the optimal recovery strategy to implement when faced with a disaster (Heng, 1996; Chow, 2000; Rapaport, 2004). Two important concepts determining maximum allowable downtime include system recovery time objectives (RTOs) and system recovery point objectives (RPOs) (definitions are contained in **APPENDIX II**). Such recovery objectives will always be defined according to the scope and nature of the interruption (Iyer and Bandyopadhyay, 2000; Pitt and Goyal, 2004; Oh, 2005). Reflecting this statement, a survey examining the backup and recovery practices of 114 companies within a variety of industries revealed that approximately less than half of the latter are confident that they can meet their RTOs using available technology (Anonymous, 2003c). Hence, it is important that all aspects of a company's recovery capabilities be taken into consideration when determining maximum allowable downtime of critical ISs. Management will be better predisposed to defend the resources required to maintain a recovery strategy when selecting these key assets (Wong, Monaco *et al.*, 1994;

Chow, 2000). **APPENDIX X** outlines these main recovery strategies in the contingency planning field.

Lee & Ross (1995) suggest a two-step evaluative method assessing system criticality by estimating the number of hours/days that business units can continue to operate without the use of critical ISs. After completing such an exercise, management can decipher critical systems from corresponding maximum allowable downtime. **TABLE 3** depicts an example of such classification:

Time without System Operations	**Degree of Criticality**
Within 24 hours	Highly Critical
Between 1 and 4 days	Critical
Greater than 5 days	Less Critical

TABLE 3 Maximum Allowable Downtime Classification (as adapted from (Lee and Ross, 1995))

CSF 11: Prioritisation of IS Applications

Lee & Ross (1995) affirm that the "most important element of an organization's replacement strategy is the prioritizing of components in case of disaster" (p.21). As such, the basic elements of a BC/DR strategy include prioritization of both critical business processes and supporting systems. (Anonymous, 2003a). Critical applications are "ISs that if damaged or destroyed, would cause significant exposure to the corporation" (Andrews, 1990, p.29). Applications affecting the ability of an organization to achieve its mission-critical objectives receive the highest priority as these recovery procedures are developed first (Rohde and Haskett ,1990, Haight and Byers, 1991; Karakasidis, 1997).

Appropriate prioritization should be established according to level of tolerance assigned by management and not to such factors as size of the IS, architecture or end-user involvement (Luecke and Hoopingarner, 1993; Wong, Monaco *et al.*, 1994; Iron Mountain, 2004). As summarized in Cerullo (1981) and Iyer & Bandyophadyay (2000), the BC/DR committee must devise a prioritization scheme to secure and protect the organization's information in a hierarchical fashion. An example is described in **TABLE 4**.

Category	Factors/Explanations
1. Critical	• Need for identical capabilities in another site • Cannot be replaced by manual methods • Usually needs to be recovered within 24 hours
2. Vital	• Need is not essential for identical capabilities in another site • Can be replaced by manual methods for a brief period of time • Usually needs to be recovered within 1 – 5 days
3. Sensitive	• No need to recover identical capabilities to another site • Can be replaced by manual methods for a defined period of time (tolerable at a certain cost) • Usually needs to be recovered within 5 – 14 days
4. Non-critical	• Absolutely no need for identical capabilities in another site • Can be interrupted for an extended period of time at no cost • Usually needs to be recovered over 14 days.

TABLE 4 Categorization of Recovery Priorities
(summarized from (Wong, Monaco *et al.*, 1994, p.30)

CSF 12: Off-Site Storage of Backup

Ensuring that all critical information, activities, systems, and material is properly backed up and stored off-site is of prime importance to the effectiveness of the BC/DR program and the continuous operation of the business when disaster strikes (Rohde and Haskett, 1990; Williams, 2002; Sun, 2004). Carlson & Parker's (1998) study of 400 US accountants in managerial positions revealed that the criteria "backup of all critical data" was the most important component of a DR plan with a 100% selection rate, followed by "restoration of data" at 98%. These two facts support the claim that backup and restoration of data is of vital importance. In another survey, 77% of respondents confirmed that their LAN data is mission-critical and employed a daily backup, with 89% of these respondents following detailed procedures (Hawkins, Yen *et al.*, 2000). In today's IT-dependent world, performing routine information and equipment backups via detailed procedures and storing them off-site through various networking means is becoming an increasing reality. Relying upon live, up-to-the-minute information is critical for corporations to sustain a competitive advantage (Jacobs and Weiner, 1997; Carlson and Parker, 1998; Sun, 2004).

As such, off-site storage of backup is critical to the functioning of the BC/DR program to the extent that "all other logistics and strategies of DRP may become meaningless" (Haight and Byers, 1991, p.15). As reiterated by Carlson & Parker (1998), "the importance of this task cannot be overstated". There exists an array of factors when discussing off-site storage of backup as described in **APPENDIX XI.** Literature on backup technologies and methods abound. The most common approaches are outlined in **APPENDIX XII**.

CSF 13: Presence of Emergency Response Procedures

To prepare emergency response procedures is an integral part of BCP/DRP and is one of the main elements of *DRII's*/*BCI's* Common Body of Knowledge (Green, 2003). These documented actions are followed immediately after a disruption to stabilize the situation (Heikkinen and Sarkis, 1996; Savage, 2002; Pitt and Goyal, 2004). These "reactive" procedures (Heng, 1996) need to be simple and clear enough to be understood by all affected staff (Msezane and McBride, 2002). Weiner (2001) affirms that well-designed emergency response procedures "must be standardized to ensure that team members respond rapidly, consistently and authoritatively to a disaster" (p.25). There should be procedures for business recovery, site restoration, crisis management, command center notification and communication procedures (Heikkinen and Sarkis, 1996; Paton, 1999; Clifton, 2000). Finally, departmental procedures, completed by the department manager, must also be documented. (Wong, Monaco *et al.,* 1994; Iyer and Bandyopadhyay, 2000).

CSF 14: Training of Recovery Personnel

The recovery effort will be futile if identified personnel are not knowledgeable and do not clearly understand their own roles and responsibilities (Morwood, 1998; Jordan, 1999; Beck, 2004) – **APPENDIX VI** lists of other articles referring to this CSF. Hence, training is a crucial element within the development stages of implementing the BC/DR program (Paton, 1999; Cerullo and Cerullo, 2004; Oh, 2005) and should be part of the BC/DR framework (AT&T, 2004). Personnel need to be kept up-to-date on the latest developments within the BC/DR plan. It is incumbent upon management to train all affected recovery personnel regarding all BC/DR procedures (Paton, 1999; Hawkins, Yen *et al.*, 2000; Lee and Ross, 1995). In fact, several studies have analyzed how on-going and evolving training heightens awareness of and lessens the potential of negative impacts from disaster

(Morwood, 1998; Paton, 1999; Clifton, 2000). Training and awareness can be communicated and taught through many educational methods, i.e., in-house training, external consulting, walkthroughs and simulations and through various media, i.e., e-mails, journals and newsletters (Rosenthal and Sheiniuk, 1993; Jordan, 1999; Zsidisin, Melnyk *et al.*, 2004). Areas to conduct the latter include new hire training, certification participation and planning methodology training (Paton, 1999; Beck, 2004; Pitt and Goyal, 2004).

Ranked as the fifth CSF within Chow's (2000) study and a key element of *DRII's/BCI's* Common Body of Knowledge, training of recovery personnel will prove to be a crucial element in BCP/DRP. Key players within a corporation need to know their roles and responsibilities when faced with a disaster. Thus, proper education and awareness are essential within the BC/DR framework.

***CSF 15**: Appropriate Backup Site*

Selecting an appropriate backup site involves prior analysis of corporate risks and business processes, determination of the criticality and degree of dependency on IT and knowledge of the length of maximum allowable downtime of critical systems (Cale and Dye, 1998; Wong, Monaco *et al.*, 1994; Chow, 2000). This ensures that all mission-critical information and equipment are appropriately safeguarded from any possible loss or damage (Iyer and Bandyopadhyay, 2000; Savage, 2002). This full recovery strategy includes preliminary measures, descriptive recovery procedures, selection of an appropriate backup site and detail of backup and off-site storage requirements of vital information and equipment (Heng, 1996; Msezane and McBride, 2002; Savage, 2002). Something as simple as a reciprocal agreement with a neighbouring company may be a perfect fit (Lethbridge, 2001).

APPENDIX X details the many recovery strategy options available when selecting an appropriate backup site. Respondents within Chow's (2000) study ranked this CSF third amongst the 18 proposed and is also one of the critical elements of *DRII's/BCI's* Common Body of Knowledge.

CSF 16: Periodical Testing of (Business Continuity/Disaster Recovery) Plan

If not thoroughly tested on a periodic and regular basis, a BC/DR plan quickly becomes obsolete (Paradine, 1995; Savage, 2002; Bielski, 2003; Oh, 2005) and can be as risky as having no plans at all (Payne, 1999; AT&T, 2004; Sun, 2004) - **APPENDIX VI** lists other articles referring to this CSF). Changes in personnel, technology, infrastructure and environment alter written procedures in some way. Consequently, testing is conducted to ensure proper documentation and maintenance (Rosenthal and Sheiniuk, 1993; Wong, Monaco *et al.*, 1994; Hawkins, Yen *et al.*, 2000).

Testing's greatest purpose is ensuring that documented contingency procedures are regularly evaluated and modified by proper recovery personnel (Wong, Monaco *et al.*, 1994; Karakasidis, 1997; Quirchmayr, 2004). This process is undertaken to confirm that all required personnel skills are updated and that all resources are aware of their responsibilities (Cerullo, 1981; Heng, 1996; Hawkins, Yen *et al.*, 2000). To affirm completeness, accuracy and reliability of the BC/DR program, a series of test programs should be developed and conducted (Heikkinen and Sarkis, 1996; Payne, 1999; (Cerullo and Cerullo, 2004). As such, numerous studies have thoroughly delineated such testing components as simulation testing (Rosenthal and Sheiniuk, 1993), testing types and program elements (Edwards and Cooper, 1995), real-life application of testing models (Laye and Torre-Enciso, 2001) and testing exercises (Payne, 1999).

Periodic and regular testing also demonstrates the ability of the business unit to recover and, conversely, of the IT service to meet the business' expectations and recovery objectives (Lee and Ross, 1995; Karakasidis, 1997; Carvajal-Vion and Garcia-Menendez, 2003). As affirmed in Cerullo & Cerullo (2004), it is no longer a matter of "if" you have to activate your plan, but "when" you will have to activate it (p.72). The resulting lessons learned are extremely valuable and motivating to all those concerned as testing is an excellent training method during which such experiences are acquired *before* having to actually face them in a live situation (Rosenthal and Sheiniuk, 1993). Nevertheless, recent surveys indicate that too many firms are ignoring the importance of contingency testing. (Anonymous, 2004c; Cerullo and Cerullo, 2004; Pitt and Goyal, 2004). Even though numbers have shown a more positive trend towards testing in recent years, corporations are not formally testing their plans on a periodic and regular basis. Consequently, it is important to conduct a thorough review and documentation of what happens. A post-mortem testing plan serves to correct any problems/deficiencies and to implement improvements (Cerullo, 1981; Rosenthal and Sheiniuk, 1993; Wong, Monaco *et al.*, 1994). As Smith (1995) states: "The three golden rules for success are (1) testing, (2) testing, and (3) testing" (p.21).

APPENDIX XIII entails some of the most common forms and approaches of testing within the BC/DR field. Ranging from pen-and-paper exercises to actual mock scenarios, management must effectively select which programs to implement and at which point of the BC/DR implementation cycle to be most effective (Arend, 1992; Castillo, 2004).

CSF 17: Maintenance of (Business Continuity/Disaster Recovery) Plan

As BC/DR plans should be tested on a regular and periodic basis, they should likewise be maintained to the same effect. Changes in technology (hardware and/or software), personnel, business strategy and the environment necessitate continuous updates of the BC/DR plan. (Arend, 1994; Paradine, 1995; Carvajal-Vion and Garcia-Menendez, 2003) - **APPENDIX VI** lists other contributions. This last phase of the BC/DR program cycle ensures that the previous completed steps – risk and impact analyses, IS prioritization, off-site storage of backup and recovery strategies, training and testing – remain as updated as possible.

When describing maintenance, a question arises: how often is often enough? A UK study revealed that 60% of companies maintained their plans annually and 20% semi-annually (Pitt and Goyal, 2004). However, 10 to 20% of a BC/DR coordinator's time is compromised by such documentation (Rohde and Haskett, 1990), consequently demanding greater time and effort from other resources as well. Hence, views differ on the subject of maintenance scheduling, yet a certain consensus emerges: volatility (industrial and organizational), corporate movement and technological advances all affect the number of times that a plan may be updated (Iyer and Bandyopadhyay, 2000). To ensure that a BC/DR plan is updated, Savage (2002) recommends developing an established schedule to be strictly adhered to and to conduct internal/external audits on a regular basis. Other documented means include control reviews, performance monitoring, simulation testing and benchmarking (Heikkinen and Sarkis, 1996; Grillo, 2003; Zsidisin, Melnyk *et al.*, 2004).

CSF 18: *Insurance Coverage for IS Loss*

The final CSF defined by Chow (2000), insurance coverage is an integral part of the BC/DR program, helping to compensate for several forms of financial loss incurred due to a catastrophe (Lee and Ross, 1995; Paradine, 1995; Savage, 2002). In essence, an effective insurance policy needs to cover all tangible and intangible costs (Luecke and Hoopingarner, 1993; Moore, 1995; Hawkins, Yen *et al.*, 2000) and successfully incorporating the latter within a properly implemented BC/DR plan may even result in reduced yearly premiums (Wong, Monaco *et al.*, 1994; Jacobs and Weiner, 1997).

Vijayaraman & Ramakrishna's (1993) study of 67 small businesses revealed that 76.1% had some insurance coverage for hardware and software loss, but relatively few (16.4%) had insurance coverage against business interruption. An extensive study conducted by Paradine (1995) fully explains business interruption (BI) insurance as a vital ingredient in a DR plan, stating that neither a DR plan nor BI insurance alone are effective to protect a company from financial loss. Thus, corporations know that they need a comprehensive BC/DR insurance policy even though executives are not excited about spending for it. Nonetheless, the entire motivation is spending pennies now instead of dollars later (Buffington, 2002).

2. Additional Critical Success Factors

Since the events of 9/11, it has been reported in the literature that other CSFs have predominated and taken on greater significance since Chow's (2000) study. Three of the most often cited are presented below.

CSF 19: Effective Communication

Communication is and has always been a vital part of the BC/DR process (Purcell, 1994; (Hawkins, Yen *et al.*, 2000; Oh, 2005). Proper communication effectively mitigates most negative impacts from disaster, prevents a disruption from becoming a full-fledged catastrophe and speeds general recovery. Successful development and implementation of a contingency plan is through communication. As such, the plan should be communicated to all affected departments and personnel (Wong, Monaco *et al.*, 1994). All policies, procedures and standards need to be communicated throughout the organization, including test results, emergency procedures and key contact information (Morwood, 1998; Sun, 2004). Knowing and understanding each individual's duties prior to a disaster occurring greatly enhances the chances of an effective recovery (Wong, Monaco *et al.*, 1994; Elliott, Swartz *et al.*, 1999).

Additionally, physical, social and financial consequences stemming from a specific disaster need to be communicated to customers, suppliers, government and public authorities (Jacobs and Weiner, 1997; Savage, 2002; Envoy WorldWide, 2005a). No greater test of corporate communication capabilities had transpired until the 9/11 attacks in New York City (Barr, 2003). All possible forms of communications, from phones, faxes, cellulars, Blackberries and e-mails were used to contact stakeholders. Consequently, communication ISs have been designed to meet the needs of such diverse stakeholders. Information access and analysis, defining priority problems, guiding emergency resource needs and providing information to managers, staff and media have become possible with these types of ISs in a real-time fashion (Paton, 1999).

CSF 20: Service Level Agreements (SLAs)

Within the BC/DR process, an important yet often neglected aspect is the negotiation, creation and management of external business and IT-related services (Vijayaraman and Ramakrishna, 1993; Pitt and Goyal, 2004; Savage, 2002). Termed service level agreements (SLAs), such documents detail business recovery requirements agreed upon by both parties (organization and external party) to be duly provided in the event of a disaster. Aspects to consider and negotiate include duration, types of services, terms and conditions, testing issues, expectations, limitations, accountabilities and storage policies (Wong, Monaco *et al.*, 1994; Smith, 1995; Karakasidis, 1997).

Moreover, importance must be given when selecting a vendor: reputation, reliability, flexibility and service offerings must be weighed when assessing the right vendor (Wong, Monaco *et al.*, 1994). Yearly reviews are thoroughly conducted to ensure that all promises are included and abided to in the legally binding document (Karakasidis, 1997). Smith's (1995) study concluded by asserting that the success of any agreement rests on the awareness, preparation, competence and confidence of all implicated personnel.

CSF 21: BC/DR Implementation Plan & Templates

Deciding to go forward with an organizational BC/DR program involves developing and presenting an effective implementation plan to the BC/DR committee or upper management. Objectives, scope, tasks, dependencies and strategy of the project are defined in such documentation (Luecke and Hoopingarner, 1993; Karakasidis, 1997; Iyer and Bandyopadhyay, 2000). Once approved, the implementation plan can be utilized to monitor and track progress of the BC/DR plan at all stages of the recovery implementation process. Monitored and administered by the BC/DR coordinator, contents of the plan include templates, work-around processes, primary contact information, notification procedures and internal/external roles and responsibilities (Karakasidis, 1997; Carlson and Parker, 1998; Cerullo and Cerullo, 2004). Template toolkits provided by external vendors can be purchased from the marketplace and adapted to meet the needs of the organization (Savage, 2002).

Consequently, developing an implementation plan involves resources from all departments working together to create a sound, effective and well-documented BC/DR plan (Wong, Monaco *et al.*, 1994; Karakasidis, 1997; Carlson and Parker, 1998). Through such means as brainstorming sessions and recovery events charting, a well thought out implementation plan can be clearly outlined and communicated to upper management (Jacobs and Weiner, 1997; Hawkins, Yen *et al.*, 2000). Benefits include consistency of BC/DR procedures, prior identification of required steps, creation of a road map for developing procedures and easier maintenance (Luecke and Hoopingarner, 1993; Clifton, 2000).

B. Business Continuity / Disaster Recovery Frameworks

Effectively implementing a BC/DR program necessitates following a specific set of industry guidelines or best practices to ensure proper implementation of all phases. Widely considered the most thorough and applicable of all BC/DR frameworks, the *Disaster Recovery Institute International* (DRII) and *Business Continuity Institute* (BCI) guidelines (DRII/BCI) define the 10 phases ("professional practices") that all practitioners should implement (Green, 2003). **APPENDIX IX** contains these practices.

Moreover, frameworks as *COBIT* (Control for Objectives, Information and related Technologies) and *ISO 17799* are best practices used as a basis for establishing a methodology of internal controls and auditing over corporate IT and related matters. Carvajal-Vion & Garcia-Menendez (2003) describe a fully-detailed comparison of these 2 specific methodologies. Through well-defined and managed IT resources and grouped processes, these frameworks help organizations balance their risks and returns in an IT environment (Grillo, 2003).

In practice, Heng's (1996) study of UK's Standard Chartered Bank (SCB) defines the methodology he used to develop BC plans. **APPENDIX XIV** depicts the methodology adopted by the bank, from planning to maintenance. According to the author, this approach is conducive to conducting an effective implementation of the BC/DR program. Karakasidis' (1997) risk reduction programme is reflected in an 11-step model as described in **APPENDIX XV**. Each component is explained by outlining its respective objectives, tasks and outcomes.

In retrospect, there exist numerous frameworks and standard practices that corporations may create, use or alter to their requirements. What is important is that the essential BC/DR steps of planning, analysis, development, implementation, testing, training and maintenance are clearly presented and defined (Pitt and Goyal, 2004). Other practices are also important to mention, but these seven steps are essential in any well respected BC/DR program.

IV. METHODOLOGY

In academic literature, authors have taken one of two classic approaches to studying empirical data: a quantitative, deductive method mostly centered around hypothesis and theory testing, or a qualitative, inductive approach focused on theory building (Yin, 1994; Newman & Benz, 1998). This has given rise to the realization that preferring one approach over another has created a "false dichotomy" as termed by Newman & Benz (1998, p.9). As such, the research methodology forwarded in this thesis report focuses on the quantitative-qualitative interactive continuum as proposed by Newman & Benz (1998).

As such, the following section will delineate how the study was conducted, using Newman & Benz's "multi-method" approach (1998). Beforehand, the main propositions will be explained and consequently analyzed to determine if the results from the multi-method research approach confirm or reject each one.

A. Main Propositions

Since Chow's (2000) study was conducted in Hong Kong amongst MIS/EDP managers actively participating in BC/DR within four industries (banking, hotel, manufacturing and trading), we believe that our Canadian-centered demographic of BC/DR experienced practitioners within four different industries (legal, banking, distribution and manufacturing) will have a greater degree of impact on the results due to factors as organizational priorities and cultural dispositions. Therefore, it is proposed:

Proposition 1: Demographic factors as country, functional role and type of industry will impact to some degree the ranking of CSFs.

Concomitantly, several years after Chow's (2000) study, it is believed that the ranking of the most important success factors have changed. The consequences of the 9/11 attacks have put into question many of the previously ranked CSFs. Throughout this paper, it has been forwarded that such corporate-based factors as training, testing and maintenance of the BC/DR program have taken on greater significance than external facets as off-site storage and alternate backup sites. Furthermore, it is postulated that the effects of the 9/11 attacks have consequently modified Chow's (2000) top 5 CSFs. However, we believe that top management commitment remains atop the list: more than ever, such a CSF is crucial in implementing an effective BC/DR program as the events surrounding 9/11 have conjured up the necessity to put people ahead of technology. As emphasized previously, much needed awareness to educate, communicate and train employees and outside stakeholders alike on the BC/DR program of an organization is thought to be of greater importance than such factors as off-site storage of backup (#4 of the top 5 as reported by Chow's (2000)) and alternate recovery site (#3 of the same study). To have a strong effect on employees, such awareness and training needs to be emphasized and supported by upper management. Therefore, the following is forwarded:

Proposition 2: The ranking of CSFs has changed due to impacts stemming from 9/11 with top management commitment continuously remaining the top ranked CSF.

Numerous disasters have occurred since Chow's (2000) study that have changed the landscape of BC/DR, none more important than the events of 9/11. New factors as communication, Service Level Agreements (SLAs) and BC/DR implementation plan have emerged that were not studied in Chow's (2000) paper that have increased significantly in importance. After analyzing the survey and interview data, we believe that the newly ranked CSFs and the additional CSFs taken together will create a new "set" of factors. As one of the main contributions of this thesis, this reduced set of constructs will aid practitioners and academics alike in determining what factors need to be implemented to possess an effective BC/DR program. We therefore propose the following:

Proposition 3: A reduced set of identifiable constructs will emanate from aggregate CSFs with newly emerging CSFs being ranked amongst the top 5 studied.

B. Multi-Method Approach

Determining research methodology depends upon such factors as the study's objectives, the type of research questions asked, the data used and the selection of data analysis techniques

(Newman & Benz, 1998). When analyzing such factors, either, or both, quantitative and qualitative methods can be applied.

Each possessing strengths and weaknesses (Yin, 1994), the multi-method approach proposed by Newman & Benz (1998) allows for a concurrent analysis of both quantitative and qualitative responses. Based on such works by Deming (1986) and Bryman (1989), it is argued that a holistic, interactive continuum between quantitative and qualitative research methods be equally analyzed and applied to get a better picture of the situation. Newman & Benz (1998) pictorially conceptualize the latter as each phase ("cell") of the process enhances the body of knowledge by building information derived from the previous cell (pp.20-21). Eventual overlaps between qualitative and quantitative cells represent the strength of using a multi-method methodology: no matter where the project is in the continuum, the feedback loop allows for a quantitative and qualitative analysis.

New & Payne (1995) also profess that the exclusive approach to conduct either qualitative or quantitative research is endemic. A trade-off is made between rigour and relevance: research that scores high on rigour may score low on relevance and vice-versa (p.61). Literature reveals that it is difficult to conduct research which conforms to the academic pattern of model building/optimizing/simulating (rigour) with the complexities of the real world (relevance) (Swamidass, 1991; Nahmias & Smith, 1994). As such, it is sometimes difficult to infer causality and to profess the straightforward process of empirical research. Hence, a mixed-methodology is sometimes warranted.

According to Newman & Benz (1998), the two approaches are neither mutually exclusive nor interchangeable. Instead, the actual relationship between the two paradigms is related to "isolated events in a continuum of scientific inquiry" (p.31). As such, we used such quantitative techniques as empirical surveys to qualitative approaches as interviews and archival data to test our propositions and answer our research questions based on such an approach (Yin, 1994; Stake, 1995).

1. Interviews

The first method of data collection was through qualitative interviews. Complementing the surveys, semi-structured interviews were conducted with eleven recovery practitioners in four distinct industries: legal (3), distribution (2), manufacturing (3) and banking (3). Each interviewee had a certain degree of understanding, working knowledge and exposure to BC/DR. A total of 10 interviews lasting about five hours were conducted with all informants. With the exception of Company C, three people were interviewed at each corporation (the former had only two people knowledgeable enough to answer BC/DR related questions). Functional roles ranged from DR specialists to senior IT managers, Interviews were conducted during a 15-week period, from April 20, 2005 to July 27, 2005. After conducting an interview, internal documentation was requested from each participant that would assist the authors in collating, synthesizing and cross-referencing responses (Schwarz & Hirschheim, 2003). Such material was given by two of the interviewees representing different organizations (Company A and B).

The interviewees were selected from a convenience sample. Even though such a small sample may be considered low and represents a self-selection bias (Nelson, 1996), interview results supplemented the one's from the survey, therefore increasing the reliability and validity of results (New & Payne, 1995).

Maturity level of a corporation's BC/DR program was based on many factors: length of time the contingency program has been in place, number of tests that have been performed (simulations or otherwise) and number of document versions of the main BCP/DRP. Some of the selected criteria were used to judge if the level BC/DR program maturity reached low, medium, high and very high. Inasmuch, each corporation represented a distinct level of maturity as reported in the next section.

The **level of analysis** of this thesis report is the organization. A major intent of the study was to determine if the impacts from the events of 9/11 had modified the ranking and selection of the top CSFs as defined in prior research to organizations (Chow, 2000). As such, practitioners were interviewed and asked questions related to such topics as current policies and procedures, benefits and drawbacks of the BC/DR initiative and driving forces to implementation of their organization. Interviewed (and surveyed) organizations represented a wide array of industries from such BC/DR mature fields as banking and insurance, to more recently BC/DR exposed fields as retail and manufacturing. With respect to interviewed organizations, these are described below.

a) Solicited Companies

Company A is the one of the world's largest producers in the mining, minerals and materials industry. With Canadian headquarters, this global manufacturer had 2003 revenues exceeding US$25 billion. Its focus on value is complemented by its commitment to the environment, health and safety and the continuous improvement of business processes. Company A is a dynamic, multilingual and multicultural organization with approximately 70,000 employees in 55 countries and regions around the globe.

Company A's BC/DR program was relatively mature compared to the other three studied as well as within the manufacturing industry in general, a sector known to have relatively low BC/DR interest. After reviewing several internal documents, it was mentioned that the DR portion had been in place since the 1980's whereas the BC initiative was implemented in the late 1990's.

Company B is one of the leading and oldest law firms to be in operations in the Canadian legal landscape. Its dedication to excellence has earned the firm an enviable reputation, both nationally and internationally. Practicing in such legal areas as business law and patent and trademarks, the firm has positioned itself to be in the forefront, pushing the boundaries to exceed expectations and deliver results to clients. With over 1200 employees in five cities, its presence has grown from a single entity to a large, legal conglomerate.

Internal documentation revealed that Company B's BC/DR program was originally initiated in March 2000, yet put on hold due to budgetary constraints at the time. After the events of September 11th, 2001, the program was re-instated and has been in full effect since March 2003.

Company C's global expansion's has rendered it one of Canada's leading distributor of motor vehicle replacement parts, tools, equipment and accessories. With over 35 years in existence, this large, multi-service corporation boasted sales volume surpassing $600 million in 2002. With more than 1,200 employees, the company has never ceased to increase and diversify its range of products, services and clientele.

Company C's BC/DR endeavour surfaced in late 2003 in response to the August 2003 blackout that affected several major Northeastern U.S. states and the Canadian province of Ontario. Even though a formal BC/DR program was not implemented, contingency measures have been in place for several years ensuring quality of service to the end customer.

With over 140 years in existence, Company D is one of the six largest chartered banks in Canada, with assets surpassing $80 billion. Its Canadian network boasts close to 500 branches. Innovation, dynamism and customer service have come to characterize the way the bank does business. Products and services for individuals and businesses alike, coupled with a non-traditional network of supermarket and offsite branches characterize this financial powerhouse.

Possessing the most mature BC/DR program from the four entities studied, Company D has thoroughly implemented, tested and maintained their separate contingency plans for numerous years. Mandated by both governments (federal and provincial) to have services recovered within a specific time period, such a process is very rigorous and all results are documented and approved by upper management.

b) Interview Process and Sample

Upon completion of the first draft of the interview questionnaire, the latter was sent to three BC/DR practitioners for initial testing (pre-test) (Hirschman, 1986; Babbie, 1989; Johnson, Leach *et al.*, 1999). Two questions (#2 and #6) were consequently modified and the questionnaire re-sent for validation. Important comments such as including leading questions, removing acronyms and phrasing questions in an easy to understand manner were incorporated. To prevent a common method bias, the selected respondent could not be selected as an interview participant (Nelson, 1996). The final version of the 3-page interview questionnaire can be referenced in **APPENDIX XVI.**

A convenience sample was used in order to ensure proper selection of candidates within the industries specified. To ensure that no self-selection bias was present, the authors first prepared to collect data by forwarding an e-mail with an attached interview consent form (see **APPENDIX XVII**) and research protocol form (refer to **APPENDIX XVIII**) advising each participant that their answers would remain confidential, their results anonymous and their participation voluntary (Yin, 1994; Fleischer & Nickel, 1995). As one of the authors completed an interview questionnaire with an interviewee, the document was forwarded by e-mail, requesting that the latter validate the information to ensure consistency and reliability of results.

After contacting each participant and validating the final version of the interview questionnaire and the two appended forms, an e-mail was sent to each of the 11 interview participants outlining the whole interview process. Upon confirmation of reading the documentation from each interviewee, a 30-minute meeting was scheduled at their convenience and preferred location (Yin, 1994; Fleischer & Nickel, 1995). Before conducting the interview, the consent form was returned duly signed and the interviewee asked if his/her answers can be tape-recorded. Upon completing the interview, the interviewee was thanked for his/her time, ensuring that all answers would remain confidential. As motivation for their involvement, a promise was made that each would receive a copy of the results once they were finalized (Bryman, 1989).

After receiving consent from all participants, each interview was transcribed by the authors from tape. To ensure response accuracy and removal of any response bias, all transcribed interviews were forwarded by e-mail and asked to be validated by the interviewee

(Eisenhardt, 1989). Once validated, all recordings were destroyed to ensure anonymity and confidentiality (New & Payne, 1995). In all cases, modifications were completed and all interviews were confirmed as accurate as possible. Finally, uniformity and consistency were ensured since the interview questionnaire acted as a guide to the interview process due to its semi-structured format (Yin, 1994).

c) Interview Analysis

Techniques as content analysis, matrices and tabular frequency of events defined the qualitative analyses used (Campbell & Stanely, 1966; Eisner & Peshkin; Lee, 1989). As defined by Miles & Huberman (1994), four main stages of the qualitative analysis process were sequentially conducted to arrive at a comprehensive result: 1) data collection, 2) data reduction, 3) data display, and 4) conclusion drawing/verification. As the data collection stage was previously described, each of the remaining 3 steps will be defined herein.

Data reduction involves the selection, simplification, and transformation of raw data into an analyzable form. As an auditing measure, a data accounting sheet was prepared defining the frequency that a specific variable was mentioned in the interview (part of this process can be referenced in **APPENDIX XXII**). Thereafter, the presentation of data into various organized forms defined the **data display** stage. As delineated in Fleischer & Nickel (1995), this task entails coding transcript sheets with a descriptive keyword process. For the purposes of this thesis, the interview text was coded according to the 21 CSFs defined therein. These groupings were defined by the authors (Foss & Waters, 2003). To ensure reliable and proper representation of data, the schema was validated by two DRIE members not participating in the survey or questionnaire (to eliminate any response bias). After all modifications were made and approved, the full schema can be referenced in **APPENDIX XIX**.

Lastly, objectivity can be assessed by the level of reliability and validity of the findings. The **Conclusion drawing /verification** phase increases the likelihood of having objective data by utilizing proven methods as checking for representativeness, content analysis and inter-rater reliability (Miles & Huberman, 1994). This last phase will be outlined when discussing the results of the study.

2. Survey

Based on Chow's (2000) methodology and findings, a structured questionnaire with a covering letter (**APPENDIX XX**) was used to collect data. Prior to sending this questionnaire, a pre-test of the survey was undertaken with two certified business continuity professionals (CBCP) ensuring that all questions were clear and simple to complete (Nelson, 1996) in addition to ensuring consistency and reliability (Hirschman, 1986; Babbie, 1989; Johnson, Leach *et al.* 1999). .Several questions reflected such organizational functions as BC/DR disasters encountered, contingency practices and critical success factors (CSFs). To prevent a common method bias, the selected respondent could not have completed the final survey questionnaire (Nelson, 1996). After such debriefing, three BC/DR practitioners completed the final survey as a post-test ensuring that all was comprehensible, rigourous and *relevant* (Benbasat & Zmud, 1999).

The final survey was answered with one of three procedures, i.e. on-line, e-mail attachment, or hard copy. The primary means of completing the survey was through an on-line questionnaire. The e-mail attachment included a cover letter as referenced in **APPENDIX XX**. The user was asked to complete the survey in its entirety and send the electronic version as an e-mail attachment to the e-mail address provided. Lastly, a hard copy of the electronic version was attached to the original e-mail requiring such the respondent to print, complete the questionnaire by hand and send it to a specific mail address.

a) Sample Population

The questionnaire was forwarded to a total of 793 *Disaster Recovery Information Exchange* (DRIE) members by all seven DRIE chapter presidents (see **TABLE 5** for more information). The latter non-profit organization represents active Canadian BC/DR practitioners. Affiliated with the *Disaster Recovery International Institute* (DRII), the governing body of BC/DR practitioners overseeing the *Certified Business Continuity*

Professional (CBCP) certification (Green, 2003), the seven participating DRIE chapters included DRIE Atlantic, DRIE Montreal, DRIE Toronto, DRIE Ottawa, DRIE SW Ontario, DRIE Central and DRIE West. Being a member in good standing of DRIE, it was given that participants actively practiced BC/DR in some capacity. Many practitioners possessed a recognized certification such as being a CBCP or a *Fellow of the Business Continuity Institute* (FBCI), but this was not mandatory to complete the questionnaire.

b) Sending Process

All documentation previously described was originally sent by e-mail to each DRIE president. E-mail instructions included the nature and reason of the survey, the deadline for submission, the three types of submissions and a sample letter to forward the previously detailed instructions to each DRIE membership. Beforehand, each DRIE president was contacted by telephone ensuring the participation of their chapter in the survey. After confirmation, the e-mail was individually forwarded to all DRIE presidents on November 1st, 2005 (please see **APPENDIX XXI** for the e-mail).

Upon reception, each DRIE president was asked to forward the survey instructions to their membership. Included in the original e-mail was a link to the on-line version and attachments to the two documents. The cover letter explained response anonymity, result confidentiality and voluntary participation. Such explanations increased the validity and reliability of the collected data (Fleischer & Nickel, 1995)

After forwarding the survey, each president was asked to submit the exact number of e-mail addresses included in the sending. This number was needed for statistical purposes. **TABLE 5** summarizes the sample population and appropriate response rates from each DRIE. Of interest is also the fact that 96.6% (87 of 90) of replies were collected trough the on-line format. From the 90 submitted responses, only 52 were usable after careful analysis since many participants omitted to answer key questions. Hence, this lowered the response rate from 11% to 7%.

DRIE Chapter	Participants Solicited	Participant Responses	Usable Surveys	Total Response Rate	Total Usable Resp. Rate
Atlantic	37	5	3	14%	8%
Montreal	142	13	9	9%	6%
Toronto	250*	32	22	13%	9%
SW Ontario	83	5	2	6%	2%
Ottawa	169	20	5	12%	3%
Central	47	8	5	17%	11%
West	65	7	6	11%	9%
TOTAL	***793***	***90***	***52***	***11%***	***7%***

TABLE 5 Demographic Sample and Survey Response Rate
(as at Dec. 1st, 2005)

LEGEND
Total Response Rate = Participant Responses / Participants Solicited
Total Usable Response Rate = Usable Surveys / Participants Solicited
(* denotes approximation since DRIE president omitted to send exact number of e-mails.).

Comprising the largest sample population, DRIE Toronto represented the greatest number of usable surveys with 22, yet the highest response rate was represented by DRIE Central with 17%, followed by DRIE Atlantic (14%) and DRIE Toronto (13%).

During the submission process, follow-ups with each chapter president were conducted bi-monthly ensuring that everything was progressing smoothly and that no problems were encountered. Furthermore, the deadline for submission was extended an extra week to Friday, December 23rd, 2005 due to the time period (Christmas holidays), giving respondents seven weeks to answer the survey.

V. DATA RESULTS

Data analysis allows linkages to be established between the research object and the outcomes regarding the original research questions (Parikh, 2002). After conducting all 11 interviews and disseminating the survey to all DRIE chapters, results were gathered, codified and analyzed to further understand how organizations effectively implemented a BC/DR program. These will be described in the following section.

A. Qualitative Results

Within four distinct industries, the BC/DR interviews were conducted with participants from different backgrounds at varying hierarchical levels in the organization. In essence, these responses supplemented the quantitative results of the study and enabled the researchers to gather a better understanding and richer depiction of what CSFs were needed in developing an effective BC/DR program. Providing an array of experiences and knowledge in regards to the corporate BC/DR initiative for their respective corporation, each interviewee had a certain degree of understanding, working knowledge and exposure to BC/DR. Although each interviewee's experience differed due to a multitude of factors, an analysis of the results indicated several common patterns.

Overall, all interviewees expressed their concern on the importance of having a BC/DR program in place at their organization. Whether it is in response to client needs or internal/external policies to quickly recover from disaster, corporate BC/DR has garnered increased importance since 9/11. A Qualitative Response Matrix revealing the most important excerpts and concepts as defined by all respondents regarding each of the six questions asked was completed (**N.B**.: The latter matrix is not included as an Appendix due to its size and since we have proceeded to include a tabular frequency table in **APPENDIX XXII**). Using the Foss & Waters (2003) quantitative coding methodology of qualitative results, key elements and concepts were highlighted, tabulated and counted according to a specific set of constructs defined by the authors (please see **APPENDIX XXII**). Passages highlighted in bold were key factors described by the participants. All underlined statements reflected important, original passages that should be included in the thesis report.

It is important to note that we had originally asked interviewees questions regarding their DR practices since we did not want to confound them with both concepts of BC and DR. However, most participants took the time to decipher the aforementioned practices distinctively. As such, the analysis below will include BC and DR answers and not solely DR as originally planned since the responses provided much value-added to the research project.

1. Interview Analysis

Upon assembling all interview information, answers to each of the six questions will be analyzed in this section. Where needed, **APPENDIX XVI** contains the original interview questionnaire.

a) Question #1

When asked how each would describe DR for their organization, most interviewees differentiated the concepts of Business Continuity (BC) and Disaster Recovery (DR) within their contingency program. They explained that BC focused on the "business side" of recovery, echoing the statement that BC represented the corporate global strategy to resume business functions. With an emphasis on stakeholders (e.g.: clients, vendors, suppliers...), an interviewee from company A iterated that "BC [...] has focused on business process and needs [...] is to show employees and clients that they are important to us." Hence, this holistic approach to recovery is defined within the global corporate environment.

Conversely, DR was reported as being the "technical focus" of firm recovery, mainly dealing with IT. Recovery of servers, infrastructure, applications and workstations were often reported throughout several interviews. As one respondent clearly noted in company B, "DR is a way to ensure that we manage the risk of losing critical systems and applications for a long period of time that may result in a substantial loss for the company."

As such, several of the corporations surveyed, especially company D, emphasized the focus on regular testing, training and maintenance.

In sum, participants were generally able to decipher the differences between both types of contingency initiatives. Regarding the importance of having a BC/DR program in place, nine of the 11 interviewees stated that BC and DR were rated at least four (4) from a 1-to-7 Likert-type scale (1 being least important), with three respondents asserting that they were extremely important, assigning a rating of 7.

b) Question #2

When asked to describe the driving forces that led to the adoption of a BC/DR program for the organization, events as "9/11", "Y2K" and "US regulations" (e.g.: SOX, HIPAA...) were emphasized by interviewees representing companies A, B and D. Furthermore, interviewees from companies B and D indicated that internal forces and policies promoted rules and regulations that must be followed regarding BC/DR. As suggested by one of the key executives from company D, "the greatest driving force was federal and provincial government regulations, followed by internal policy".

Nonetheless, a force that was mentioned by only one of the companies (C) as being a key driving factor was the August 2003 blackout. Indeed, driving forces can be attributed to many factors, yet none was more important than 9/11 and US regulations, partially confirming our second proposition.

c) Question #3

With respect to current policies and procedures in place since the initial implementation of a BC/DR program, information varied between organizations. Nonetheless, corporations with well-developed, tested and maintained BC/DR plans as companies B and D were better able to detail these BC/DR policies and procedures than those with relatively new contingency programs (companies A and C). Very detailed hierarchies and chain of command structures within company B, represented by such entities as an IT Council and an Audit Committee, are critical to effectively implementing a proper BC/DR program.

The same can be said about company D's alternate recovery sites and thorough testing process. Despite this, both corporations with no formal policies and procedures iterated that these are "currently being worked upon" (company A) or "will be so in the foreseeable future" (company C).

Supporting the importance of having well developed BC/DR procedures, the events of 9/11 certainly impacted to some degree the policies and procedures defined within each interviewed corporation. Statements as 9/11 "triggered the development and official implementation of various DR[BC] plans" (company B), "heightened the sense of urgency to develop policies and procedures" (company D) and "shed light and put BC/DR plans back in the spotlight" (company A), these assertions echoed the importance that 9/11 had on organizational development. Even though company B had plans in place prior to 9/11 and interviewees reflected that the latter event had no real effect on the policies and procedures at the time, one of the resources questioned noted that "9/11 put more emphasis on making sure that we deliver an effective BC/DR strategy than ever before." Hence, such statements further support our second proposition that 9/11 did have an impact on organizations.

d) Question #4

Frequency and resource requirements related to BC/DR initiatives greatly varied amongst corporations. For example, company A had one assigned resource dedicated to the BC/DR function working with approximately 20 part-time contributors. BC/DR was discussed once, "maybe" twice a year at the upper management (Executive Committee) level. However, company B's response was centralized on various committees. Higher level committees (e.g.: IT Council, Audit and IT P&P) met on a quarterly basis, whereas BC/DR plant-based resources met on a monthly basis. Moreover, committees represented approximately five to seven individuals, whereas dedicated plants had a single representative for each location. A global corporation, company B had five dedicated BC/DR resources, with approximately 100 worldwide individuals having some degree of implication within the BC/DR project.

Thus, it is important to note that even though some organizations as company C do not possess a dedicated full-time resource to BC/DR and some are even partially outsourcing BC/DR functions (company D), all interviewed organizations revealed that the BC/DR issue was discussed at least once a year and that several resources worked on this endeavour in some capacity. Thus, such facts demonstrate the increased importance of BC/DR on the corporate agenda since the events of 9/11.

e) Question #5

As with any other corporate initiative, benefits and drawbacks emerge and it is vital to understand and decipher these within the stated project. Some of the most interesting testimonials included benefits as "being organized" (companies A and B), "being in control" (company A), "quicker response time" (company A), "rigour" (company B), "credibility" (company D) and "piece of mind" (company D). As one interviewee succinctly stated, "BC/DR allows us to ensure that we can provide uninterrupted service to our clients." Hence, the greatest benefits of BC/DR are not only favorable to the organization, but ultimately to the stakeholder as well.

Conversely, stated drawbacks from interviewees revolved around two central themes: financial cost and human effort. Maintaining, testing, training and implementing are all phases within the BC/DR process that incur great expense and resource time. As reported by one of the interviewees, "the biggest drawback is keeping the BC/DR plan up-to-date." Nonetheless, participants believe that the benefits outweigh the costs as organizations reap the rewards upon recovery.

f) Question #6

The most important question within the interview process required interviewees to describe that main BC/DR factors attributable to an effective recovery program. This final question was meant to collect factors that were the most critical and determine if these have changed since Chow's (2000) study. Without going into great detail, common factors found within Chow's (2000) study included IS prioritization of applications (CSF#11), top management support (CSF#1), adequate financial support (CSF#2), and business impact analysis

(CSF#9). Despite the latter, the more intriguing and revealing factors were comprised of a new set of factors that we have termed "intrinsic". Such concepts described within the interviews included:

- "Commitment";
- "Remaining calm";
- "Knowing one's roles and responsibilities";
- "Client response";
- "Member safety"; and
- "Communication"

Thus, the above partially supports our stated third proposition. As best formulated by an executive at company A: "Whatever happens as a whole is a better indicator of success than meeting pre-defined recovery objectives," further asserting that "real success will be assessed after the disaster."

2. Quantitative Analysis of Interview Results

A quantitative study of the qualitative statements made from the eleven participants was conducted after determining the criteria to be used in doing so. **APPENDIX XXII** shows this analysis in a Matrix format.

The most cited CSF amongst the 21 studied (Chow's 18 CSFs and the three additional included by the authors) was testing, with a frequency of 39. Repeated 11 times within the first question by four of the respondents alone, the importance of testing cannot be underscored. Companies B and D have conducted pre-defined and regular tests for many years and such a process has since been instilled in their BC/DR process and culture ever since. In addition, company D is even mandated by federal and provincial authorities to conduct such tests on a semi-annual basis to ensure that stakeholders' needs are immediately addressed upon a disaster occurring. Thus, the interviews clearly reveal the level and importance of testing.

Maintaining BC/DR plans was the second most quoted CSF within the collected interviews. Even though constant and regular maintenance was mostly referred to as a drawback of implementing a BC/DR program (Question #5), several interviewees acknowledged that such a process needed to be an integral part of possessing an effective contingency program. As paraphrased from an interviewee's answer in company B, having the BC/DR initiative properly maintained allowed a more effective recovery of all essential services after the events of 9/11. As such, maintenance has garnered increased importance since Chow's (2000) study as revealed during the interviews.

Training of recovery personnel was mentioned 11 times during the recorded interviews, representing the third mostly referred CSF. Likewise increasing in importance since Chow's (2000) study (training was ranked 5th in the latter), this factor was mostly alluded to upon questioning current policies and procedures in place since the initial implementation of a corporate BC/DR program (Question #3). As such, training is revealed to be an essential component of a BC/DR initiative, ensuring that implementation is effectively conducted through personnel being educated on their roles and responsibilities. Supporting this claim, company A's three participants all mentioned to some extent the significance and effect of training on the BC/DR design. Thus, as important as it was within Chow's (2000) study, training remains atop the most essential CSFs.

Surprisingly, external consulting was the fourth most cited CSF, with a frequency of 10. Outsourcing a part of the BC/DR function to a third party was mentioned to some extent by many interviewees. To varying degrees, the use of external consulting ranged from having an initial analysis completed by an outside firm (company A) to thoughts of outsourcing the entire BC/DR function (company C). Even though such a factor was not mentioned within Chow's (2000) top 5 CSFs, corporations are increasingly looking towards outsourcing this secondary function, focusing their efforts on their core business practices.

Lastly, impact analysis rounded out the top 5 cited CSFs in interviews. Revealed nine times, participants explained that this factor was an integral part of their current policies and procedures since initial implementation of the contingency program (Question #3). Respondents from company B defined an impact analysis process that all plants must undertake. Thoroughly defined by one of the latter's interviewed resources, the "four levels of DRP" are based upon the impact assessments of a system. The latter company utilized impact analysis in 2004 to define all mission-critical functions for all Business Units (BUs). This was conducted since the company wanted to "clarify all BUs degree of risk and uncertainty" when faced with disaster. Hence, impact analysis' usefulness stems from the crucial function of assessing the repercussions that a disaster may have upon an organization, rendering it one of most critical factors in a BC/DR program. **TABLE 6** below shows the summary of the quantitative count above.

A word count of the pre-defined variables above was tabulated as per **APPENDIX XXII**. Consequently, a visual representation of the top 5 cited CSFs within the interviews as delineated above is found below in **TABLE 6.**

CSF		COUNT
Periodical testing of BCP/DRP	(CSF16)	39
Maintenance of BCP/DRP	(CSF17)	15
Training of Recovery Personnel	(CSF 14)	11
Engagement of Recovery Consultant	(CSF 7)	10
Business Impact Analysis (BIA)	(CSF 9)	9

TABLE 6 Top 5 cited Critical Success Factors as per Interview Variable Count

In sum, the quantitative analysis of the qualitative results has revealed a widespread degree of importance within certain factors in a post 9/11 world. Through the six questions in the interview questionnaire, the ranking and most often cited CSFs differed substantially from Chow's (2000) study, concentrating more on such BC/DR based phases as testing (CSF#1 within this study), maintenance (CSF#2) and training (CSF#3). Inasmuch, these results partially support our second and third propositions, adding greater support and validity to the claim that internal corporate practices have replaced the more external facets of a BC/DR program.

B. Quantitative Results

Survey results reveal important trends that confirm several stated propositions. Before delving into the numbers, the processing of quantitative data is elaborately described. Pursuant to the latter, descriptive statistical analysis of the 28 questions will be conducted, followed by an exploratory analysis of results using SPSS.

1. Survey Process and Sample

A preliminary step to analyze survey data is ensuring that all submitted responses are properly entered. To be as accurate and objective as possible, all hard copy versions (three documents total) were entered electronically by one of the authors as the other validated their entry (Fleischer & Nickel, 1995).

Upon downloading the summarized results from the survey provider's website, all close-ended, multiple-choice questions were organized into an Excel spreadsheet. Open-ended questions were thereafter categorized, analyzed and codified according to relevance of results. To reduce systematic response bias, Nelson & Cooprider (1996) suggest combining responses for certain questions. This would provide measures containing less unique variance. Hence, aggregating responses would be less affected by haphazardous guesses to specific questions. For instance, job titles given in Question #3 were grouped according to level of management (e.g.: executive, middle, staff and consultant) and if they were BC/DR related. For this specific question, responses were grouped and categorized under seven different headings, allowing easier classification and consequent analysis of results.

The first part of the questionnaire (Q1 to Q9) sought a description of the respondent (e.g.: DRIE chapter, job title, etc.) and organizational details (e.g.: industry, number of employees, etc.). This was followed by specific questions on triggers, types and specific aspects of the main BC/DR program (Q10 to Q24). Interrogations as "When did your firm decide to implement a BC/DR program?", "How often do you test your BC/DR program?"

and "In your opinion, do employees get sufficient BC/DR program related training at your location?" represent some questions. Lastly, the final four questions were related to Chow's (2000) CSFs, in addition to several not mentioned therein. Anchoring survey questions in the domain of study as well as in past research increases reliability and validity of results (Silk, 1982; Markus and Lee, 1999).

Since only 52 of the 90 respondent questionnaires were usable, this low response rate can be attributed to the limitations and complexities of the on-line version (Many questions required all options to be answered. If the participant omitted to answer one or more of the options to a particular question, the system did not allow the respondent to submit the survey, yet all answers were registered in the database despite the latter), the timing of the survey (sent during the Christmas holidays), and length of the attached questionnaire (10 pages).

Normally, a consequence of a low response rate is that it introduces a self-selection bias (Nelson & Cooprider, 1996). However, since the survey was directed at Canadian DRIE members in good standing, it was impossible to direct the documentation to a specific cross-section of practitioners or industries in particular. Therefore, results can be generalizable, removing any issue of self-selection bias (New & Payne, 1995).

2. Descriptive Statistics

The first nine (9) survey questions required respondents to answer specific demographic details regarding their BC/DR practice and organization. Personal questions as DRIE membership (Q1) and job title (Q3) revealed that most of the 52 usable responses were represented from the DRIE Toronto chapter (22 participants) and most practitioners came from Middle Management (41 respondents).

From an organizational perspective, the main industries represented within the sample of 52 (Q2) were from the public/parapublic (12 of 52), financial other than banking (10) and technological (8) sectors. Compared to Chow's (2000) restrictive study within four industries (manufacturing, hotel, banking and retail), participants in this study worked within eleven. Hence, generalization of results can be extended since the latter are more representative of a broader range of industries than in Chow's (2000) study. As such, our first proposition (that country, functional role and type of industry will impact to some degree the ranking of CSFs) is fully supported.

Within the corporation, 71% of solicited respondents (37 of 52) indicated that there were less than 3 full-time employees (Q4). This is representative of previous BC/DR surveys asking similar questions (Envoy WorldWide, 2005b; KPMG & Continuity Insights, 2006). Not surprisingly, the upper executive level (e.g.: CEO, CFO, CIO...) was reported as the most effective champion of the BC/DR program in the organization (56%) followed by the managerial level (e.g.: directors, managers, supervisors...) at 37% and the operational level as BC/DR planners, coordinators and administrators representing 7% (Q5). Statistically, location size (Q7) was distributed mostly between 100 and 500 employees (31%) with an identical percentage representing locations comprising between 500 and 1000 resources. On the other hand, organization size (Q8) can be categorized as medium to large, with 37 of 52 respondents working in organizations with greater than 1000 employees. Respondents in previous BC/DR surveys have likewise tended towards the larger size organization than the small-to-medium sized based businesses (e.g.: SMEs) (KPMG & Continuity Insights, 2006).

The two remaining demographic-based questions dealt with the existence of different BC and DR programs in the same organization (Q6) and budgetary BC/DR related expenses (Q9). With respect to the former, results were somewhat evenly distributed between three selections, with most organizations revealing that they implemented a mixture of both programs (40%). Conversely, half of respondents indicated that local operational expenses dedicated to BC/DR expenses were less than 1%, while 29% replied that they did not know the exact percentage of local operational expenses dedicated to the BC/DR program. The remaining 21% of responses varied between 1% to greater than 5% of operating expenses.

Hence, results from this section of the survey are aligned with similar surveys conducted within the field as mentioned previously, supporting the assertion that the results can be increasingly generalizable.

3. Specific BC/DR Questions

The remainder of the questionnaire focused on specific BC/DR related issues. Without delving into great detail, the most important answers will be further explained below.

a) Questions 11 to 14: Issues regarding BC/DR implementation

Questions regarding implementation of the BC/DR program comprised such issues as level of cooperation (Q10), timing (Q11), reason for implementation (Q12), impact(s) since implementation (Q13) and policies (Q14). Worthy to mention are the facts that

- management implication comes from various levels in the corporation (upper, middle and lower) and not only from a single defined department as IT or an external source as a consultant;

- thirty-two of the 52 respondents (62%) worked in organizations possessing mature BC/DR plans greater than six years old (prior to January 1st, 2000);

- of particular interest is the fact that a majority of respondents indicated that their organization initially developed a BC/DR program because of some other event than Y2K, 9/11 or US regulations, thus partially refuting our second proposition. Sixty-three (63) percent mentioned such corporate-specific events as best practices (5 respondents cited this factor), a technological failure (4 respondents), or risk assessment/analysis (3 respondents). Conversely, more widespread disasters as the August 2003 blackout were cited as a driving factor of creating a BC/DR program;

- existing contingency programs were predominantly unaffected by any of the important events in the last decade postulated to have an impact on the current BC/DR initiative.

Over two-thirds of the survey sample indicated that Y2K, 9/11 and US regulations did not influence the current contingency program in place, further negating the proposition that surrounding events of 9/11 impacted the ranking of CSFs;

- finally, internal policies were not given any more importance by respondents than were external policies. Thirty of the 52 respondents, or 58%, refuted internal policy influence on BC/DR related decisions, a percentage to close to state any conclusion with certainty.

Thus, our claim that key events as 9/11, Y2K and US regulations had had a definite impact on organizations was not fully supported from the results of the survey, despite having strong assertions in the interview. As mentioned further on, further research would have to be conducted to understand such opposing results.

b) Questions 15 to 20: Most common types of BC/DR disasters

When asked about any type of data loss suffered due to such catalysts as natural catastrophes (Q15), accidental (Q16) and intentional (Q17) human disasters and intentional (Q18) and accidental (Q19) technological mishaps since January 1st 2004, a majority of the participants indicated that their organization did not suffer from any type of the aforementioned disasters. The most specified types of disasters were technological (23 of 52 respondents cited such types of disasters) and natural (22 of 52). Most often cited examples included power outages (14 of 52), computer viruses and worms (10) and hardware failure (8). Delving into greater detail, participants who indicated that they were consultants or working within a consultancy firm (as asked in Q3) experienced a majority of these disasters.

As such, the results may be indicative of an ever-increasing reality: corporations, despite being prepared, have not experienced any real calamitous event to test their BC/DR plans. Supporting this assertion was the fact that respondents indicated that the total cost of such events (Q20) was reportedly less than $100,000 (23%) More disturbingly, approximately half reported that no cost was incurred whatsoever (48%).

c) Questions 21 to 24: Recovery assessment

BC/DR documentation related inquiries regarding recovery assessment spanned such issues as procedures (Q21), objectives (Q22 and 23) and performance (Q24).

With respect to recovery procedures used to assess recovery, departmental tests (62%), alternate site business resumption (62%), crisis emergency/management (58%) and mock disaster management (56%) were mostly utilized by corporations. Three of the aforementioned procedures are internally-focused (alternate site business resumption being the exception). As iterated previously, corporations are increasingly relying on such internal -based components as testing, training and education to assess recovery rather than externally centered factors as alternate site recovery and redundant facilities. This fact partially supports our third proposition that a new set of factors has emerged since 9/11.

Ranking the recovery objectives of budget, time and business priorities (Q22), it was clearly evident from the data that business priorities were the most critical with 85% of the respondents ranking this factor above all else. Time was ranked as being the second most important with 83% supporting that this factor should be placed second to business recovery. Lastly, 85% of participants reported budget as being the last recovery objective of those proposed. In essence, **TABLE 7** below depicts participants' selection:

REC. OBJECT. / RANKING	**1st** (out of 52 respon.)	**2nd** (out of 52 respon.)	**3rd** (out of 52 respon.)
Budget	2	6	44
Time	6	43	2
Business Priorities	44	3	5

TABLE 7 Ranking of Recovery Objectives

After careful analysis of the data, three types of business priorities were defined: keeping core business requirements operating as much as possible during a disaster (14 of 44 respondents), continuing to provide customer/client satisfaction (11 of 44) and ensuring health and safety of employees (4 of 44). As evidenced in the interviews, organizationally-centered priorities are considered just as critical as recovery within time and budget. Such objectives were identical across intra-organizational boundaries (58%), emphasizing that recovery objectives were the same irrespective of location (Q23).

When measuring performance of the BC/DR program (Q24), the top factor selected was plan exercises, with 43 respondents (or 83%) utilizing this form of performance measurement. Second closest measure was audit findings, with 29 participants (or 56%) indicating that they used this specific technique. As such, performance criteria were mostly centralized around "intrinsic"-based phases as testing and auditing, once again partially supporting the claim of the emergence of a new set of factors (proposition #3).

d) Questions 25 to 27: Testing, Maintenance and Training: The Big Three

Questions regarding testing (Q25), maintenance (Q26) and training (Q27) were consequently asked. Most respondents surveyed indicated that the BC/DR program was tested on an annual basis (37%), yet a majority maintained surrounding documentation semi-annually (35%). Of particular interest is the fact that very few organizations have never tested or maintained their BC/DR program: less than 4% of respondents indicated such. This favorable trend is indicative of the growing popularity of BC and DR in organizations. Taking the time to properly test and update the various BC/DR documents is a sign of best practices within the industry.

Despite the above, respondents felt that employees did not receive sufficient BC/DR related training in their respective organization: 37 of the 52 respondents – 71% – of BC/DR practitioners surveyed attested to the latter claim. This is an alarming percentage that needs to be addressed through such practices as awareness programs (e.g.: lunch and learns, newsletters, BC/DR sponsored sessions, quarterly e-mails, etc.) and proper education.

e) Q1 to Q27: Summary

In sum, from the 52 respondents that completed the entire questionnaire, the survey has partially supported several stated propositions. Despite such issues as little exposure from actual disasters and unsatisfactory BC/DR related training programs, respondents have indicated that corporations are using BC/DR best practices as pre-establishing recovery objectives, contingency performance measures, testing and maintenance effectively. As such, a new set of factors has emerged, emphasizing "intrinsic" related BC/DR components as testing, training and maintenance over "extrinsic" factors as alternate recovery sites and data backup procedures.

f) Questions 28 to 32: Post-Chow info.

Some of the most important contributions of this study address the topics of importance level and ranking of the top five Critical Success Factors (CSFs). The first two questions (Q28 and Q29) questioned the level of importance of Chow's (2000) 18 CSFs and the ranking of the top five in order to determine if the ranking has changed since Chow's (2000) study. Similarly, new factors emerging from this study were consequently assigned a level of importance (Q30) and ranked amongst the previous 18 (Q31) to determine if there exists a possibility to create a new top 5 ranking, possibly confirming our third proposition.

g) Question 28: Level of importance attributed to each CSF

As posited, top management support was given the highest level of importance from the 18 CSFs as defined in **APPENDIX XXII**, with 32 of the 52 respondents (62%) emphasizing that this factor was "Extremely" important to their corporate BC/DR program. Lagging behind was maintenance of the BC/DR program with 44% support and Business Impact Analysis (BIA) rounded out the top 3 within this category at a 38% selection rate. Interesting was the composition of the most selected factors reflecting "Very" important factors to implement in a BC/DR program. Eleven from the 18 CSFs had at least 25 respondents underlining this level of importance. Examples include participation of representatives from each department with 33 respondents choosing that this factor was very important, followed by IS applications prioritization with a response rate of 60% (31 representatives) and training of personnel not far behind with 56% support.

In brief, it is interesting to note that engaging an external consultant (CSF7) was deemed to be "Less" (15 of 52 respondents) and especially "Not at all" (18 of 52 respondents) important to a BC/DR program, contrary to the interview results that revealed it was the fourth most cited CSF. A similar trend was also noted for insurance coverage for IS loss. In our report, it was important to analyze how off-site storage of backup (CSF12) and appropriate backup site (CSF15) fared since these were posited to be less important than more "intrinsic" factors as training, maintenance and testing. With a mean hovering around the "Very" level of importance, it is difficult to fully conclude that these factors were less important than others.

In sum, "intrinsic" CSFs as maintenance, training and most often cited top management support were predominately important, largely supporting our second and third propositions. Consequently, "harder" based factors as backup sites and offsite storage were important to a lesser extent and external factors as consultants and insurance coverage were much less crucial.

h) Question 29: Ranking of 18 CSFs in a post-9/11 world

Using Chow and Luk's (1996) proposed ranking methodology, **APPENDIX XXIII** reveals the top five CSFs from the answer to Q28. As posited in our second proposition, top management support still remained the #1 ranked CSF with 73% of respondents indicating that this factor should be prioritized as the most critical CSF. The 2nd ranked factor proved to be Business Impact Analysis (BIA), slightly edging alignment of corporate goals with company objectives, which proved to be immediately ranked third amongst the 18 factors. The fourth and fifth factors were maintenance and testing of the BC/DR program respectively.

Analyzing the above, the top 5 CSFs have differed substantially from Chow's (2000) original study conducted six years ago. **TABLE 8** below shows the results of this analysis, lending support our second proposition.

CSF		RANK
Top Management Support	(CSF 1)	1
Business Impact Analysis (BIA)	(CSF 9)	2
Alignment of BC/DR Obj .with Comp. Goals	(CSF 3)	3
Maintenance of BCP/DRP	(CSF 17)	4
Periodical Testing of BCP/DRP	(CSF 16)	5

TABLE 8 Top 5 cited Critical Success Factors as per Survey Ranking Methodology Proposed by Chow & Luk (1996)

i) Question 30: Possible additional factors

Pursuant to the questions regarding the level of importance and ranking of Chow's (2000) 18 CSFs, several new factors have emerged since the events of 9/11 that warrant further study. Three factors deemed important to implement in a BC/DR program from supporting literature were effective communication, inclusion of Service Level Agreements (SLAs) and the existence of a BC/DR implementation plan. In a similar vein as was conducted with the 18 CSFs, the level of importance and ranking amongst the previous 18 CSFs of Chow's (2000) study was requested.

From the 52 valid respondents, 33 (or 63%) rated effective communication as being "Extremely" important with an additional 18 (or 35%) expressing that this was "Very" important to have in a BC/DR program. Conversely, SLAs were predominantly ranked as being "Somewhat" important. Interestingly, the existence of a BC/DR implementation plan was assessed as being "Very" important, with a response rate of 54% (28 respondents).

As described above, effective communication held the most importance in terms of level and ranking. Would the latter hold with other CSFs? As such, one of the final remaining questions asked to rank the three CSFs along with any other important CSF not mentioned in the report (NOTE: due to insufficiency of reported results, the ranking of any other factor than the 21 mentioned was not considered. Nonetheless, **TABLE 9** delineates some of the most important answers given by several participants). Of the 35 respondents who answered this optional question, 18 mentioned that effective communication was deemed "Extremely" important to implement. Hence, this further supports our assertion that new factors have appeared since Chow's (2000) study, adding greater evidence and partially support our third claim.

OTHER CSFs	LEVEL OF IMPORTANCE
Crisis Management	Extremely
Contacts lists (team members and vendors)	Extremely
Spokesperson training	Somewhat
Incident Management	Very
Collaboration with external organizations	Very

TABLE 9 Examples of Other Critical Success Factors Mentioned by Survey Participants not Found in Chow (2000) or Current Survey Questionnaire.

C. Exploratory Analysis & Results

To increase validity and reliability of results, further exploratory analysis was conducted on the quantitative data to determine if there was (were) a new set(s) of CSFs that possibly emerged since the events of 9/11. Through SPSS, factor analysis was conducted to uncover any new patterns from collected data. As will be explained below, such an analysis has generated interesting results.

APPENDIX XXIV shows and explains the generated Component Matrix tables through various iterations of the 18 CSFs. Each iteration reflects the goal of having the highest Cronbach alpha (α) with respect to a particular set of components. Items (in our case, CSFs) were removed if the stated α was negative or if its removal increased the alpha for other components within that reduced set of factors. As such, there are four basic sets of factors that can be further studied after conducting five iterations on the data (see

APPENDIX XXIV – FINAL ITERATION). Each one will be subject to interpretation in the following section.

1. Factor sub-set #1: Business Continuity / Disaster Recovery "Intrinsic" Factors

The first factor set described in **APPENDIX XXIV** groups four CSFs that have a substantial degree of correlation (Cronbach α = .8031). Periodic testing of BCP/DRP (CSF16; α = .772), training of recovery personnel (CSF14; α = .752), maintenance of BCP/DRP (CSF17; α = .725 and presence of emergency response procedures (CSF12; α = .626) represent what we have hypothesized to be the set of factors that have gained greater importance since the events of 9/11. We have termed such a set "intrinsic" since these factors represent key attributes within the BC/DR internal program that involve participation of critical resources within the organization and represent key phases within the BC/DR program. This is especially relevant of the first three CSFs represented in this set since these comprise the final three phases of a BC/DR initiative.

2. Factor sub-set #2: Business Continuity / Disaster Recovery Personnel Requirements

The first sub-set illustrates two CSFs, perfectly correlated (Cronbach α = 1.0000), comprising personnel issues that must be initially addressed before commencing a BC/DR program. Participation of representatives from each department (CSF6; α = .877) The presence of a formal recovery planning committee (CSF5; α = .877) and are interdependent. Industry best practices recommend that corporate participation in a "formal" recovery planning committee should comprise representatives from each department in order to be able to better respond to any type of disaster. Hence, it is implicit that a formal recovery planning committee be comprised of representatives from all departments, rendering these two CSFs perfectly correlated.

3. Factor sub-set #3: Business Continuity / Disaster Recovery Analysis Process

The third factor set as defined in **APPENDIX XXIV** consolidates the determination of maximum allowable downtime (CSF10; α = .813) and prioritization of IS application (CSF11; α = .779) with business impact analysis (BIA) (CSF9; α = .713). The latter represents a common tool used within a BC/DR initiative with the other two well known results documented from the aforementioned tool in the BC/DR plan. All factors of this subset can be categorized as factors pertaining to the BC/DR analysis process (Cronbach α = .7610). Logically, a BIA culminates in such documentation as a system/application maximum allowable downtime chart and an IS applications prioritization schema, summarizing an important part of the BC/DR process.

4. Factor sub-set #4: Business Continuity / Disaster Recovery Managerial Issues

Categorizing the three CSFs of adequate financial support (CSF2; α = .836), alignment of BCP/DRP objectives with company goals (CSF3; α = .659) and top management support (CSF1; α = .627) into a common set, the relationship between these facets suggests managerial components that must be implemented in a BC/DR program (Cronbach α = .6936). Financial, strategic and organizational support must be decided from the outset before effectively implementing a corporate BC/DR initiative. It is interesting to underline that top management support, despite having some degree of importance within this specific set, did not possess the highest α within the set (adequate financial support encompassed a higher α of ,836). Thus, partial substantiation was held for the second proposition. In essence, this set of managerial factors entails financial aid and managerial collaboration, corporate alignment of goals, all factors deemed crucial prior, during and after implementation.

5. The unapparent sub-set: Business Continuity / Disaster Recovery "Extrinsic" factors

A missing set of factors not illustrated in **APPENDIX XXIV** classifies two often related BC/DR factors when implementing a BC/DR program: offsite storage of backup (CSF13) and the selection of an appropriate backup site (CSF15). Despite this association, the lack of importance may reflect the fact that these factors are not as important as reported in Chow's (2000) study. Hence, this assertion adds further support to the claim that "intrinsic" factors as training, testing and maintenance of a BC/DR program are of greater significance since the events of 9/11. Inasmuch, extrinsic factors, although still required in a BC/DR initiative, have lost the lustre of the days when storage, applications and data dominated over people and processes.

6. Conclusion

The exploratory factor analysis using SPSS confirms a majority of the applicable propositions. Lending support to the third proposition, a new set of factors has emerged, classified under the headings of BC/DR intrinsic factors, personnel requirements, analysis process and managerial issues. Such a classification can be attributed to the events of 9/11 having shaken the contingency planning field and the practitioners that operate therein. Focus has shifted from applications, storage and data-based factors to resources-driven aspects as personnel and organizational priorities. It is therefore incumbent upon academics and practitioners alike to take advantage of this information, tailoring the BC/DR program to effectively handle these new factors.

VI. CONCLUSION/DISCUSSION

As can be evidenced from the preceding results, all emerging CSFs from this study have an organizationally-centered base. We termed these as "intrinsic" factors since they are representative of internal corporate practices. Conversely, Chow's (2000) study has revealed that two of the five factors are externally-oriented to the corporation, with the third and fourth being what we term as "extrinsic" factors. Hence, as posited in our second proposition, Chow's (2000) CSFs have changed and consequently modified the priorities of organizational recovery. This is evident as new CSFs have surfaced and been prioritized accordingly within the top five, concomitantly supporting our third proposition.

	Top 5 CSFs in Chow's study	**Top 5 CSFs in Current Interview Study**	**Top 5 CSFs in Current Survey Study**
RANK	***CSF***	***CSF***	***CSF***
1	Top Management Support	Periodical Testing of BCP/DRP	Top Management Support
2	Adequate Financial Support	Maintenance of BCP/DRP	Business Impact Analysis (BIA)
3	Appropriate Backup Site	Training of Recovery Personnel	Alignment of BC/DR Objec. with Company Goals
4	Off-site Storage of Backup	Engagement of External Consultant	Maintenance of BCP/DRP
5	Training of Recovery Personnel	Business Impact Analysis (BIA)	Periodical Testing of BCP/DRP

TABLE 10 Comparison of Critical Success Factors between Chow (2000) and Current Survey and Interview Studies.

As such, the variety of results derived from the interviews and survey questionnaire can be somewhat confusing if not properly summarized. As such, **TABLE 11** below depicts the confirmation / rejection of a particular proposition within a specific type of analysis.

PROP. ANALYSIS	**Qualitative Analysis**		**Quantitative Analysis**	
	Interview Analysis	*Quantitative. Anal. of Interview Results*	*Descriptive Statistics*	*Exploratory Analysis (SPSS)*
Proposition #1	*N/A*	*N/A*	FS	*N/A*
Proposition #2	**PS** (9/11 effect)	FS (9/11 effect)	**NS** (9/11 effect)	*N/A* (9/11 effect)
	N/A (top 5 CSFs Δ)	**PS** (top 5 CSFs Δ)	FS (top 5 CSFs Δ)	**PS** (top 5 CSFs Δ)
Proposition #3	*N/A* (new CSF in top 5)	FS (new CSF in top 5)	FS (new CSF in top 5)	*N/A* (new CSF in top 5)
	PS (reduced set of CSFs)	*N/A* (reduced set of CSFs)	**PS** (reduced set of CSFs)	FS (reduced set of CSFs)

TABLE 11 Confirmation/Rejection of Proposition According to Type of Analysis

LEGEND: FS = Fully Supported; **PS** = Partially Supported
NS = Not Supported; *N/A* = Not Applicable
Items in bold denote Partial or No support

A. Interpretation of Proposition Support/ Non-support

From the table above, it is safe to say that a majority of the propositions were confirmed, partially or fully, within all types of analyses. In particular,

- The first proposition regarding impacts of country, functional role and/or industry type on the ranking of CSFs was objectively supported solely within the statistical survey analysis since questions were specifically asked regarding such issues. Interviews did not clearly explore this proposition, yet some logical extrapolations can be made regarding given answers. For example, respondents from company D stressed testing to a great degree, whereas company A's focus was on management support. We believe that it is safe to say that given cultural, social, economical and political circumstances, CSFs will greatly differ from one country, industry, organization and individual to the next. The Asian business landscape circa 1999 is much different now and should be more so upon comparing regions within the Middle East, Africa and North America.

- Strikingly, the second proposition was not fully supported within the survey data as it was within many interviews regarding the after-effects of 9/11 on the BC/DR program. Other factors were revealed to alter the current BC/DR program yet certain interviewees, as in companies A and B, confirmed that 9/11 did have some degree of impact due to these events and consequently on their top CSFs. However, we cannot fully state that there was an immediate correlation between the changes in CSFs and the impacts from 9/11. Further research would need to be conducted solely on this issue to see if this was the case.

- As described in **TABLE 10**, it was evident from the results of the qualitative and quantitative analyses that the top five ranked CSFs have changed since Chow's (2000) study. Yet these analyses seem to have contradicted one another since results from the quantitative analysis of interview results and statistical SPSS revealed another prime CSF than top management support. Only after analysis of the descriptive statistics from the survey that top management support was deemed to be the top CSF. As such, we can conclude that the top CSFs have been modified, excluding the assertion that top management support remains as the top CSF.

- Fully supported within the third proposition was the speculation that new CSFs will be ranked within the top five. In both quantitative and qualitative analyses, effective communication was an excellent example of a newly stated CSF that was not mentioned within Chow's (2000) study that was emphasized as being very important. In fact, many participants who answered the optional question requesting a new ranking of new CSFs amongst Chow's (2000) eighteen suggested effective communication as being in the top 5. Thus, future research may be conducted to study the effects of new CSFs on BC/DR initiatives.

- Lastly, a reduced set of factors was indeed evident upon conducting further statistical analysis. Through SPSS, generated results revealed four reduced sets of factors that were consequently analyzed. As posited throughout the report, "intrinsic" factors as training, testing and maintenance were given more importance than "extrinsic" factors as offsite storage of backup and an appropriate backup site, which were not even included in the reduced set. Thus, the growing importance of "intrinsic" factors has many academic and practical implications, of which will be described in the forthcoming section.

B. Summary: What We Have Learned

Hence, the strengths of the multi-method approach are described above, as both qualitative and quantitative analyses lend support to substantiate reliability and validity of results and confirm a majority of our propositions. Even though both qualitative and quantitative sample sizes were relatively small, it is still noteworthy to mention that results tended to confirm each other. As delineated throughout, such confirmations increase generalizability and reliability of results.

VII. LIMITATIONS

All research possesses some degree of limitations in collecting, analyzing, interpreting and disseminating information. This section describes a couple of the most revealing within our examination of the topic at hand.

- The greatest limitation in the research process was geographical scope. Interviewees were selected from a convenience sample, representing Quebec resources implicated to some degree in their BC/DR corporate program. Survey respondents, on the other hand, were representative of a very large subset of active Canadian BC/DR practitioners. Hence, results can be somewhat skewed since answers within interviews might have differed throughout other Canadian provinces. For instance, legislation in one province substantially can affect BC/DR business practices, resulting in discrepancies between provinces. Likewise, survey answers might have been different if participants would have been only selected solely from the DRIE-Montreal chapter. Hence, validity of results can be violated if geographical scope was not maintained across data collection methods.

- Sample size was also another easily identifiable constraint. With a sample size of 11 interviewees and 52 usable responses, an argument might be that the sample size in both cases is not representative enough of the Canadian BC/DR landscape, limiting the generalizability of proposed findings. Yet we argue that since this is a multi-method approach to conducting research, both analyses complemented one another, reducing variability and inconsistency of results.

VIII. IMPLICATIONS

The results discussed previously can have major implications to both academic and practitioner communities. Each of the latter will be discussed in greater detail in the following section.

A. Academic Implications

Confirming the main research question of this paper, a major academic contribution of this report reflects the assertion that events of 9/11 have impacted to some degree the implementation of BC/DR initiatives. Even though quantitative responses partially support the latter, interviewees clearly stated that 9/11 has impacted corporate BC/DR implementations. Such a revelation has significant academic implications since analysis would need to be adapted to integrate the impacts stemming from events of September 11th, 2001. For instance, BC/DR academics increasingly need to consider the human/resource perspective upon formulating conclusions as opposed to a hardware/equipment centered focus since people have been deemed to be more vital in the recovery process than physical equipment or data. Hence, studying and analyzing BC/DR issues is no longer contained at the data/tools level: personnel issues need to be considered before rendering a final conclusion.

Furthermore, statistical analysis confirmed a reduced set of factors that may have significant repercussions to academic groups. Knowing this reduced set of factors, researchers may use these to conduct further research. Such future study can be pursued looking at a specific set or analyzing all four components. In essence, the reduced set of factors aid academic researchers in understanding what specific constructs lead to a particular proposition being supported or not supported.

Consequently, the three most revealing CSFs from all 21 mentioned represent three of the most important phases of the BC/DR implementation process. Testing, training and maintenance were rated significantly higher in terms of criticality, relevance and impact since the events of 9/11 within quantitative and qualitative studies than such CSFs as an appropriate backup site and offsite storage. The latter two CSFs, deemed extremely critical in prior research, have given way to the aforementioned CSFs. As such, "intrinsic" factors – testing, training and maintenance – comprising a reduced set of factors and being ranked amongst the top 5 CSFs, have become the focus of BC/DR programs.

Another academic implication stemming from this report is the results and consequences of using a multi-method approach to conduct research. By having qualitative data support quantitative analysis, research reliability and validity are increased. Academically, having a small sample population is purported to lessen credibility and validity of results, yet drawing similar conclusions from two different research analyses increases such criteria. Hence, this study proves that using both quantitative and qualitative methods substantiates research results.

B. Practitioner Implications

Of equal importance is the capability of research results to be applied to the business community. Implications for BC/DR practitioners abound, the most revealing and applicable ones described below.

The greatest implication from results described in this report is the effect that the latter would have on current BC/DR programs. Contingency professionals will be inclined to review their current BC/DR plans in light of the research results described. For instance, the reduced set of factors confirmed through statistical analysis impacts to a certain degree the importance given to specific contingency measures. As emphasized throughout this report, appropriately termed "intrinsic" CSFs as testing, training and maintenance have taken greater importance than "extrinsic" concepts as offsite storage and selecting an appropriate backup site. Such facts question the contents of current BC/DR programs since past research has shown to emphasize extrinsic factors over intrinsic topics. Hence, practitioners need to be put greater emphasis on "intrinsic" BC/DR – especially since the events surrounding 9/11 – due to people becoming the greatest corporate asset of the 21st century as emphasized in the literature and study participants.

Consequently, added emphasis needs to be put on people in the organization. Without diminishing the criticality of data to the corporation, resources have been deemed ever-critical to recovery. Evidenced by the fact that literature and survey participants underlined the lack of BC/DR related training in the industry, all resources – from key executives to lower-level staff – need to understand their roles and responsibilities when confronted with a disaster. As such, practitioners need to be aware of such reality and adjust their communication plan accordingly. Without people, recovery cannot occur.

Consequently, practitioners need to adapt their training/awareness techniques as an effect of such results. Training material needs to specifically address personnel issues as recovery tasks and responsibilities, procedures, key processes and functional roles as opposed to offsite locations and alternate sites. Thus, knowing what to do, when to do it and how to proceed when recovering must be communicated in an easy-to-follow, succinct manner, ensuing that resources grasp all concepts and steps along the way.

In essence, it is particularly important to understand and accept all implications stemming from the results of current research. In this thesis report, we have detailed the most important and revealing factors for practitioners and academics alike. It is common practice to analyze the recommendations given to better comprehend what repercussions results of this research might have on all affected parties.

IX. FUTURE RESEARCH

After conducting this study, many avenues of research are readily apparent that are interesting to pursue. Some of the most intriguing are:

- New CSFs that have gained significant importance since the events of 9/11 can comprise a research paper altogether. Since the current study sought to determine if CSFs from prior research hold true in a post 9/11 world, assessing the importance of new CSFs was not a prime objective. Since the final two questions of the survey questionnaire addressing new CSFs were optional, many answers were left blank. A thorough analysis of the collected data could not have been determined without compromising reliability and validity of results. Hence, emerging CSFs as effective communication and BC/DR plan implementation can encompass two of many CSFs that are reported to be extremely important in today's environment and see if the ranking amongst newly proposed CSFs alter prior research standings.

- Surprisingly, quantitative analysis was contrary to qualitative examination regarding the degree of impact stemming from the events of 9/11. In the former, survey participants did not fully support the significance occurring from the events of 9/11, yet interviewees were more adamant, stating that 9/11 certainly modified their current BC/DR initiative. Thus, this area of confusion can be subject to further scrutiny by academic researchers, specifically addressing how 9/11 altered current BC/DR practices.

- The low training rate reported within interviews and surveys certainly is another area of further academic research. Questions as to the reasons for such a low rate, whether low training is pervasive amongst all industries or simply certain areas and methods for instilling training in corporations is a subset of topics that can be further studied. Being one of the top 5 CSFs in this study, further analysis into this CSF remains an important field of future research.

- An important area that we omitted to ask survey participants within the demographic section of the survey (first nine questions) was their status as BC/DR practitioners. It would be interesting to know if most of the participants were certified in the BC/DR domain (e.g.: CBCP, ABCP, FBCI, MBCI…) as well as to know under which administrative function they reported to (e.g.: IT, HR, Building services…). Results from such questions can give us a better understanding of how well our sample population understood and practiced BC/DR.

- In a similar vein as above, other demographic factors as years of experience, level of expertise and tenure in a corporation within BC/DR can also be studied. These would also add value to research results as they can give better insight to the typical BC/DR respondent profile.

- After careful analysis, an interesting area of future research would be to cross-reference the maturity level of an organization's BC/DR program with the top CSFs found within this study. Are highly matured organizations more inclined to focus on strategic, intrinsic factors as testing, training and maintenance than less matured corporations? Are less matured organizations more susceptible to be influenced by corporate, extrinsic factors as top management influence and adequate financial support? Such questions can be answered through a well-driven analysis of maturity level and selected reduced sets of constructs.

- Lastly, the first proposition posited that variables as country, functional role and type of industry will impact to some degree the ranking of CSFs. Since the survey was solely conducted throughout Canada and the interviews carried out in Quebec, an area of future research would be to see if the same results would be simulated in other parts of the world, especially in the US. As the events of 9/11 occurred in New York, it would be ideal to investigate if the results of this study would be replicable. In addition, this study looked at four specific industries other than those conducted in Chow's (2000) study. Future research can examine if other industries will reveal the same level of impact stemming from the events of 9/11 on their current BC/DR program.

X. BIBLIOGRAPHY

Alonso, F. and J. Boucher (2001). "Business Continuity Plans for Disaster Response." The CPA Journal **71**(11): 60.

Andrews, W. C. (1990). "Contingency Planning For Physical Disasters." Journal of Systems Management **41**(7): 28-32.

Anonymous (2003a). Expecting the Unexpected: CFO Survey Finds Not All Companies Have Disaster Recovery Plans in Place (Press Release), Robert Half Management Resources. **2005**.

Anonymous (2003b). One in Three US Companies Operate Without a Formal IT Disaster Recovery Strategy, Continuity Central. **2005**.

Anonymous (2003c). "Survey Reveals Disaster Recovery Expectations and Reality." Information Management Journal **37**(6): 8.

Anonymous (2004a). Inside the Numbers: Facts and Figures on the State of Business Continuity. Continuity Insights**:** 1.

Anonymous (2004b). Inside the Numbers: Facts and Figures on the State of Business Continuity. Continuity Insights**:** 1.

Anonymous (2004c). Three Years Later: Many Businesses Still Unprepared After 9/11. Continuity Insights**:** 1.

Archivas (2004). "Digital Archiving Strategies for Regulatory Compliance in Financial Services (White Paper)." 1-8.

Arend, M. (1992). "Data Processing Report: Disaster Preparation Beats Disaster Recovery." ABA Banking Journal **84**(12): 40-42.

Arend, M. (1994). "Time to Dust Off Your Contingency Plan." ABA Banking Journal **86**(2): 56-58.

AT&T (2004). "Achieving Resilience - Best Practices in Business Continuity (White Paper)." 1-7.

Babbie, E. (1989). The Practice of Social Research. Belmont, CA, Wadsworth Publishing.

Bandyopadhyay, K. and L. L. Schkade (2000). "Disaster Recovery Planning by HMOs: Theoretical Insights." Health Care Management Review **25**(2): 74-84.

Barr, J. (2003). "A Disaster Plan in Action: How a Law Firm in the World Trade Center Survived 9/11 with Vital Records and Employees Intact." Information Management Journal **37**(3): 28-29.

Beck, E. (2004). Measuring Risk: Laying the Foundation to Justify BC Investment. Continuity Insights**:** 36-41.

Berman, M. (2005). "The Good, the Bad and the Really Ugly - from an IT Perspective." Sarbanes-Oxley Compliance Journal(March): 5.

Bielski, L. (2003). "Business Continuity Planning Must Step Up." ABA Banking Journal **95**(11): 52-54.

Bielski, L. and S. Cocheo (1999). "Is Your Contingency Plan All That It Can Be?" ABA Banking Journal **91**(4): 45-51.

Booker, R. (2004). "Cyber Security & Business Continuity Planning." Pipeline & Gas Journal **231**(3): 14-16.

Botha, J. and R. Von Solms (2004). "A Cyclic Approach to Business Continuity Planning." Information Management & Computer Security **12**(4): 328-337.

Bryman, A. (1989). Research Methods and Organization Studies. London, EN, Unwin Hyman.

Buffington, J. (2002). "Business Continuity." Computer Technology Review **22**(12): 32-33.

Buffington, J. (2003). "How to Partner for Disaster Recovery." Computer Technology Review **23**(4): 23, 36.

Buffington, J. (2005). "Data Replication: A Key Element in BCP (Part of the ILTA 2005 White Paper series)." ILTA: 13-15.

Burgener, E. (2004). Assessing the Foundation of Long Distance Disaster Recovery. Computer Technology Review. **24:** 24-25.

Bryman, A. (1989). Research Methods and Organization Studies. London, EN, Unwin Hyman.

Cale, D. A. and C. B. Dye (1998). "Why Disaster Recovery Plans Are Usually Not Adequate." Ohio CPA Journal **47**(1): 37-38.

Campbell, D. and J. Stanely (1966). Experimental and Quasi-Experimental Design for Research. Chicago, IL, Rand McNally Publishing.

Cardona, A. (2003). "Contingency Planning and the HIPAA Security Rule." Disaster Recovery Journal **16**(3): 6.

Carlson, S. J. and D. J. Parker (1998). "Disaster Recovery Planning and Accounting Information Systems." Review of Business **19**(2): 10-15.

Carvajal-Vion, J.-F. and M. Garcia-Menendez (2003). "Business Continuity Controls in ISO 17799 and COBIT." Upgrade: European Journal for the Informatics Professional **4**(6): 17-23.

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

Cerullo, M. J. (1981). "Accountants' Role in Computer Contingency Planning." The CPA Journal **51**(1): 22-26.

Cerullo, V. and M. J. Cerullo (2004). "Business Continuity Planning: A Comprehensive Approach." Information Systems Management **21**(3): 70-78.

Chalaka, R. (2003). Simplifying Disaster Recovery Solutions to Protect Your Data. Computer Technology Review. **23:** 36.

Chandler, R. C. and J. D. Wallace (2004). "Survey: Business Continuity Planning after September 11." Disaster Recovery Journal **17**(3): 8.

Chow, W. S. (2000). "Success Factors for IS Disaster Recovery Planning in Hong Kong." Information Management & Computer Security **8**(2): 80-86.

Chow, W. S. and V. W. S. Luk (1996). "Management in the 1990's: a Comparative Study of Women Managers in China and Hong Kong." Journal of Managerial Psychology **11**(1): 10h.

Chudnow, C. (2001). Disaster Recovery -- Not if You Need It, but How to Do It. Computer Technology Review. **3rd Quarter:** 52-55.

Clifton, R. W. (2000). "Business Continuity Planning." Occupational Health & Safety **69**(10): 178-180.

D'Antoni, H. (2003). Business Continuity Slides Down the Priority Scale. InformationWeek. **922:** 1.

Davis, C. K. (2004). "Planning for the Unthinkable: IT Contingencies." Information Management **17**(3/4): 2-4.

Deming, W. E. (1986). Out of the Crisis. Cambridge, MA, Center for Advanced Engineering Study, MIT.

Dixon, J. E. and T. K. Murphy (1994). "Creating Emergency Programs for Business Disaster Recovery: The Case of Dade County, Florida." Economic Development Review **12**(3): 45-48.

DM Review (2005). Glossary (definition of Critical Success Factor), DM Review. **2005**.

Dow, J. (2004). "Disaster Recovery: Regulatory Issues." Computer Technology Review **24**(4): 32.

DRI International (2006a). DRII Glossary. **2006**.

DRI International (2006b). Professional Practices for Business Continuity Professionals, DRI International. **2006**.

DRJ (2003), Glossary of Business Continuity/Disaster Recovery Terms, DRJ. **2006.**

Edwards, B. and J. Cooper (1995). "Testing the Disaster Recovery Plan." Information Management & Computer Security **3**(1): 21-33.

Edwards, M. (2003). Image Backup & Disaster Recovery. Computer Technology Review. **23:** 18-19.

Eisner, E. and B. Peshkin (1990). Qualitative Inquiry in Education. New York, NY, Teachers College Press.

Eisenhardt, K. (1989). "Making Fast Strategic Decisions in High-Velocity Environments." Academy of Management Jounal **32**: 543-576

Elliott, D., E. Swartz, *et al.* (1999). "Just Waiting for the Next Bang: Business Continuity Planning in the UK Finance Sector." Journal of Applied Management Studies **8**(1): 43-60.

Envoy ENS (2006). Enterprise Notification Services, Envoy World Wide. **2006**.

Envoy WorldWide (2005a). Conducting a Critical Communications Audit: Four Steps to Ensuring Continuity of Business Communications (White Paper). Bedford ,MA**:** 12.

Envoy WorldWide (2005b). Trends in Business Continuity and Risk Management: Business Continuity Survey. Bedford, MA**:** 8.

Faile, C. and D. Mucisko (2005). Corporate-Wide Business Continuity and Disaster Recovery Plans Jump 20 Percent in Last 5 Years: Deloitte & Touche LLP Survey (Deloitte & Touche LLP Press Release). New York City, NY**:** 2.

Ferelli, M. (2002). Business Continuity Drives D2D Backup. Computer Technology Review. **22:** 1-2.

FEMA (2001). US Major Disaster Declarations between January 1, 1972 and December 31, 2000, FEMA. **2006.**

Fleischer, C. S. and J. R. Nickel (1995). "Attempting TQM in Organizational Staff Areas, TQM as Managerial Innovation in Corporate Public Affairs." Canadian Journal of Administrative Sciences **12**: 116-127.

Foss, S. K. and W. Waters (2003). Coding & Analysis of Qualitative Data. **2006.**

Garvey, M. J. (2004). Behind the Numbers: Businesses Brace for Disruptions. InformationWeek**:** 2.

Gibson, S. (2005). Sarbanes-Oxley: In Search of Payback. eWeek**:** 3.

Green, W. G. (2003). Certification in Business Continuity. Partners In Emergency Preparedness Conference, Seattle, WA.

Grillo, A. (2003). "Information Systems Auditing of Business Continuity Plans." Upgrade: European Journal for the Informatics Professional **4**(6): 12-16.

Haight, N. and C. R. Byers (1991). "Disaster Recovery Planning: Don't Wait Until It's Too Late." Journal of Systems Management **42**(4): 13-16.

Hane, P. J. (2001). Update: More Disaster Recovery Resources. Information Today. **18:** 14-15.

Hanna, G. (2005). "Disruptions Needn't Spell Disaster (Part of the ILTA 2005 White Paper series)." ILTA: 7-9.

Hawkins, S. M., D. C. Yen, *et al.* (2000). "Disaster Recovery Planning: a Strategy for Data Security." Information Management & Computer Security. **8**(5): 222-229.

Heikkinen, D. and J. Sarkis (1996). "Disaster Recovery Issues for EDI Systems." Logistics Information Management **9**(6): 27-34.

Heng, G. M. (1996). "Developing a Suitable Business Continuity Planning Methodology." Information Management & Computer Security **4**(2): 11-13.

Hensley, P. and W. Zane (1998). Liquidity Contingency Planning for Y2K. Credit Union Executive Journal. **38:** 12-13.

Hirschman, E. (1986). "Humanistic Inquiry in Marketing Research: Philisophy, Method and Criteria." Journal of Marketing Research **23**(8): 237-249.

Hood, S. B. (2005). Always Be Prepared: 10 Ways to Know if You're Ready for Any Disaster. Canadian Business**:** 3.

Iron Mountain (2004). The Business Case for Disaster Recovery Planning: Calculating the Cost of Downtime (White Paper). Boston, MA**:** 8.

Iyer, R. J. and K. Bandyopadhyay (2000). "Managing Technology Risks in the Healthcare Sector: Disaster Recovery and Business Continuity Planning." Disaster Prevention and Management **9**(4): 257-267.

Jacobs, J. and S. Weiner (1997). "The CPA's Role in Disaster Recovery Planning." The CPA Journal **67**(11): 20-25.

Johnson, J. (2005). "Corporate Compliance Challenges and Escrow Management." Sarbanes-Oxley Compliance Journal **16**(9): 6.

Johnson, W., P. Leach, *et al.* (1999). "Theory Testing Using Case Studies in Business-to-Business Research." Industrial Marketing Management **28**(3): 201-213.

Jordan, E. (1999). "IT Contingency Planning: Management Roles." Information Management & Computer Security **7**(5): 232-238.

Karakasidis, K. (1997). "A Project Planning Process for Business Continuity." Information Management & Computer Security **5**(2): 72-78.

Kenniston, S. (2005). "What is Compliance, Really?" Sarbanes-Oxley Compliance Journal: 2.

Klein, L. (2005). Sarbanes-Oxley and Outsourcing : Time is Running Out for Non-US Companies. Continuity Central**:** 4.

KPMG & Continuity Insights (2006). A Review of the Factors Influencing Business Continuity Management Programs - FINAL REPORT**:** 25.

Laye, J. E. and M. I. M. Torre-Enciso (2001). "Strategies to Reduce the Impacts of Disasters on Business Processes: The Case of Business Continuity." International Journal of Risk Assessment and Management **2**(3/4): 319-329.

Lee, A. (1989). "A Scientific Methodology for MIS Case Studies." MIS Quarterly **13**(1): 33-50.

Lee, S. and S. Ross (1995). "Disaster Recovery Planning for Information Systems." Information Resources Management Journal **8**(3): 18-23.

Lethbridge, N. (2001). Impact of Information Warfare on Business Continuity Planning. 2nd Conference of Information Warfare & Security, Perth, Australia.

Lim, D. (2003). Disaster Recovery. Asia Computer Weekly**:** 1.

Luecke, R. W. and C. Hoopingarner (1993). "Business Continuity Planning: The Hospital's Insurance Policy." Healthcare Financial Management **47**(4): 30-36.

Markus, M. L. and A. S. Lee (1999). "Special Issue on Intensive Research in Information Systems: Using Qualitative, Interpretive, and Case Methods to Study Information Technology." MIS Quarterly **23**(1): 4.

Marlin, S. (1999). Regulators Stress Need for Contingency Planning. Bank Systems & Technology. **36:** 10.

McCracken, A. (2005). Unravelling Business Continuity Terminology, Continuity Central.

Mendoza, A. (2004). "Business Continuity and ILM." Computer Technology Review **24**(8): 8-11.

MessageOne (2006). AlertFind Enterprise. **2006**.

Michaels, A. S. (2005). Terms (definition of Critical Success Factor). **2005**.

Miles, M. and A. Huberman (1994). Qualitative Data Analysis: An Expanded Sourcebook. Thousand Oaks, CA, Sage.

Moore, P. (1995). "Critical Elements of a Disaster Recovery and Business/Service Continuity Plan." Facilities **13**(9/10): 22-27.

Morwood, G. (1998). "Business Continuity: Awareness and Training Programmes." Information Management & Computer Security **6**(1): 28-35.

Msezane, T. and J. McBride (2002). "Corporate Real Estate and Business Continuity: An Integrated Enterprise Conceptualisation." Journal of Corporate Real Estate **4**(4): 348-356.

Nahmias, S. and S. A. Smith (1994). "Optimizing Inventory Levels in a Two Echelon Retailer System with Partial Lost Sales." Management Science **40**(5): 582-596.

Nahum, N. (2003). Cost-Effective Disaster Recovery. Computer Technology Review. **23:** 36-37, 47.

Nelson, K. (2000). A Contingency Model of IT Disaster Recovery Planning. Proceedings of the 2000 Americas Conference on Information Systems (AMCIS), Long Beach, CA.

New, S. J. and P. Payne (1995). "Research Framework in Logistics: Three Models, Seven Dinners and a Survey." International Journal of Physical Distribution & Logistics Management **25**(10): 60-77.

Newman, I. and C. R. Benz (1998). Qualitative-Quantitative Research Methodology: Exploring the Interactive Continuum, Carbondale & Edwardsville.

Oh, M. (2005). "Business Continuity: What is the Right Fit for your Firm? (Part of the ILTA 2005 White Paper series)." ILTA: 3-5.

Padilla, R. (2005). Don't Gamble with HIPAA Security Compliance. TechRepublic**:** 2.

Paradine, P. J. (1995). "Business Interruption Insurance: a Vital Ingredient in your Disaster Recovery Plan." Information Management & Computer Security **3**(1): 9-17.

Parikh, M. (2002). "Knowledge Acquisition Through Case Study Development: A Student Researcher Perspective." Communications of the AIS **8**(8): 360-379.

Paton, D. (1999). "Disaster Business Continuity: Promoting Staff Capability." Disaster Prevention and Management **8**(2): 127-133.

Payne, C. F. (1999). "Contingency Plan Exercises." Disaster Prevention and Management **8**(2): 111-117.

Peffers, K. and T. Ya (2003). "Identifying and Evaluating the Universe of Outlets for Information Systems, Research: Ranking the Journals." The Journal of Information Technology Theory and Applications **5**(1): 22.

Perez, J. C. (2005). Gartner: Security Concerns to Stunt E-Commerce Growth. Computerworld**:** 3.

Perry, S. (2004). "Survey: Most EMEA Countries Unprepared for a Disaster." Computerworld **38**(48): 1.

Pisselo, T. (2002). "How Much Is Enough?" Disaster Recovery Journal **16**(1): 29-31.

Pitt, M. and S. Goyal (2004). "Business Continuity Planning As a Facilities Management Tool." Facilities **22**(3/4): 87-99.

Price, E. (2002). "Disaster Recovery for Collaborative Environments." Computer Technology Review **22**(5): 19.

Pumo, B. S. (2004). "Contingency Planning: Are You Ready for the Unexpected?" Journal of Health Care Compliance **6**(3): pp.45-47.

Purcell, L. (1994). "L.A. Banks All Shook Up, But Disaster Recovery Worked." Bank Systems & Technology **31**(3): pp.36-37 (2 pages).

Quirchmayr, G. (2004). Survivability and Business Continuity Management. Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation, Dunedin, New Zealand.

Rapaport, G. (2004). Preparing for Disaster with an Effective Business Continuity Strategy. Computer Technology Review. **24:** 30-31.

Riley, P. (1999). "Strategies for Y2K Contingency Planning." Computer Technology Review **19**(8): 26-27.

Robinson, S. (2002). Disaster Recovery: Redefining Disaster Recovery as 24x7. Computer Technology Review. **22:** 30.

Rockart, R. F. (1979). "Chief Executives Define Their Own Data Needs." Harvard Business Review **57**(2): 81-93.

Rodriguez, T. (1997). Wide-Area Data Mirroring Protects Business Continuity. Storage Inc.**:** 47-48.

Rohde, R. and J. Haskett (1990). "Disaster Recovery Planning for Academic Computing Centers." Communications of the ACM **33**(6): 652-657.

Rosenthal, P. H. and G. Sheiniuk (1993). "Business Resumption Planning: Exercising the Disaster Management Team." Journal of Systems Management **44**(6): 12-16; 38-40.

Savage, M. (2002). "Business Continuity Planning." Work Study **51**(4/5): 254-261.

Scalet, S. D. (2001). The ABCs of Disaster Recovery. CIO**:** 2.

Scarinci, C. (2002). "Contingency Planning for Small Businesses." The CPA Journal **72**(8): 65.

Smith, R. (1995). "Business Continuity Planning and Service Level Agreements." Information Management & Computer Security **3**(3): 17-21.

Sugano, A. (2005). 10 Steps to Building a Sound Disaster Recovery Plan. Windows IT Pro**:** 5.

Sun (2004). Business Continuity, Corporate Survival, and Liability. Questions and Answers for the Senior Executive (White paper). Santa Clara, CA**:** 23.

Surmacz, J. (2001). Disaster Plans Lacking. CIO. **15:** 1.

Swamidass, P. M. (1991). "Empirical Science: New Frontier in Operations Management Research." Academy of Management Review **16**(4): 792-814.

Schwarz, A. and R. Hirschheim (2003). "An Extended Platform Logic Perspective of IT Governance: Managing Perceptions and Activities of IT." Journal of Strategic Information Systems(12): 129-166.

Verton, D. (2003). Study: Many Companies Lack Disaster, Continuity Plans. Computerworld. **37:** 1.

Vijayaraman, B. S. and H. V. Ramakrishna (1993). "Disaster Preparedness of Small Businesses with Micro-Computer Based Information Systems." Journal of Systems Management **44**(6): 28-32.

Vogl, G. J. (2005). Management of Information Systems: Glossary of Terms (definition of Critical Success Factor). **2005**.

Watson, S. (2004). How to Steer Your Company to Emergency Preparedness in Nine Steps. Continuity Insights**:** 4.

Weiner, S. (2001). "Managing Effective Disaster Recovery." The CPA Journal **71**(12): 22-26.

Williams, N. (2002). "Balancing the Needs of Data Storage and Business Continuity." Computer Technology Review **22**(1): 16.

Wilson, B. (2004). Which Came First - Business Continuity or Disaster Recovery? Continuity Insights**:** 2.

Wong, B. K., J. A. Monaco, *et al.* (1994). "Disaster Recovery Planning: Suggestions to Top Management and Information Systems Managers." Journal of Systems Management **45**(5): 28-33.

XOSoft (2004). Preparing for an Effective Business Continuity Strategy (White Paper). Burlington, MA**:** 6.

Yin, R. (1994). Case Study Research: Design and Methods. Thousand Oaks, CA, Sage Publications.

Zsidisin, G. A., S. A. Melnyk, *et al.* (2004). An Institutional Theory Perspective of Business Continuity Planning for Purchasing and Supply Management. 89th Annual International Supply Management Conference, Anderson School at UCLA.

APPENDIX I Business Continuity / Disaster Recovery Alarming Quotes

A *Gartner Inc.* study revealed that 40% of businesses that experience a major incident and do not have a recovery plan in place will be out of business within 12 months (Wilson, 2004;XOSoft, 2004).

BCI (*Business Continuity Institute)* estimates that only 60% of organizations have disaster and recovery plans, with only 25% having been renewed to reflect the changing nature of the organization (Elliott, Swartz *et al.*, 1999).

Two-thirds of BC professionals surveyed in a recent Deloitte & Touche LLP study indicated that their company does not possess enterprise-wide BC programs (Faile and Mucisko, 2005).

Of the 1,259 IT professionals polled by *Dynamic Markets* within EMEA (Europe, Middle East and Africa) countries, 16% do not have a recovery plan in place, 34% have not gotten around it and 24% said that they do not need one. A greater preoccupation is the finding that 97% of businesses surveyed would be unable to continue normal operations following a data center fire (Perry, 2004).

In a study released by *Dataquest*, 17% of the 205 IT managers interviewed from end-user companies said that they do not intend to develop a BC/DR plan and 30% said that they were considering it. (Verton, 2003).

In 2001, Gartner estimated that, on average, 40% of network downtime is caused by application failures, 40% by human error, and 20% by environmental or system failures (AT&T, 2004).

Nearly 1 in 3 companies from a sample population of 202 IT directors surveyed by Imation Corp. are operating without of formal DR strategy in place. (Anonymous, 2003b).

APPENDIX II Business Continuity / Disaster Recovery Terminology

Examples & Types of Disasters

TYPES / EXAMPLES & SOURCE
• Natural disasters • Fires, earthquakes, lightning, storms and static electricity; • Software malfunctions; • Hardware or system malfunctions; • Power outages; • Computer viruses; • Man-made threats • Vandalism, hackers, and sabotage; and • Human error, • Improper computer shutdown, spilling liquids on the computer and cigarette ash. (Hawkins, Yen *et al.*, 2000)
• Natural disaster; • Sabotage; • Vandalism; • Riots; • Bombing threats; • Air conditioning failure; • Personnel unavailability; • Hardware failure or destruction; • Operating system failure; • Database management system failure; • Power failure; • Operating errors; • Building collapse.
• Natural disasters • Fire • Floods • Earthquakes • Normal crises; business accidents related to • Personnel • Work stoppages • Loss of key employees • Vandalism • Workplace violence • Physical events

TYPES / EXAMPLES & SOURCE

        - Industrial accidents
        - Supply-chain breakdowns
        - Product failures
    - Economic events
        - Hostile take-overs
        - Recessions
        - Bankruptcies
- Abnormal crises
    - Criminal events
        - Product tampering
        - Acts of terrorism
        - Kidnappings
        - Fraud
    - Informational events
        - Cyber-attacks
        - Theft of company proprietary info.
        - Tampering with company records
    - Branding events
        - Logo tampering
        - Misuse of branding in merchandising and trademarks
        - Slander

(Cerullo and Cerullo, 2004, p.17)

Categories of Disasters

CATEGORIES OF CBIS DISASTERS

HUMAN		**NON-HUMAN**
ACCIDENTAL	*DELIBERATE*	
Misplacing	Theft	Fire damage
- Software	- Hardware	Water damage
- Data	- Software	Property damage
- Documentation	- Data	Power surges
- Supplies	- Supplies	
	- Documentation	**DUE**
Erasing (data/software)		**TO**
- By users	Sabotage	
- Machine failure	- Hardware	Earthquakes
	- Software	Floods
Bad modifications	- Data	Lightning
- Data	- Supplies	Tornados
- Software	- Documentation	Ocean waves
- Documentation		Snow
	Tampering	Hurricanes
System glitches	- Software	Dust storms
- Hardware	- Data	Ice storms
- Software	- Documentation	Cold weather
		Hot weather
Power disruption	Employee	Cyclones
	- Absences	
Fire	- Termination	
Computer virus	Power disruption	
	Computer virus	

(taken from (Vijayaraman and Ramakrishna, 1993, p.29, **Table I**)

Definitions of Disaster

DEFINITION & SOURCE
"[...] an event that is likely to cause significant disruption in an organization's operations for a period of time." (Chow, 2000, p. 80)
"[...] any event that can cause a significant disruption in the information services capabilities for a period of time and affect the operation of the organization." (Chow, 2000, p. 80)
"[...] an interruption in the availability of a CBIS [Computer Based Information System] when there is a need for it for business purposes." (Bandyopadhyay and Schkade, 2000, p.75)
"[...] an event that halts the critical business functions within an organization." (Hawkins, Yen *et al.*, 2000, p.229)
"[...] an interruption of mission-critical information services for an unacceptable period of time." (Nelson, 2000)
"Activities and programs designed to return the entity to an acceptable condition. 1) The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions" (DRI International, 2006a)
"[...] any event that causes significant disruption to operations, thereby threatening the business' survival." (Rohde and Haskett, 1990, p.652; Rosenthal and Sheiniuk, 1993, p.13)
"[...] anything that interrupts normal business activity." (Robinson, 2002, p.30)
"A sudden, unplanned calamitous event which results in a great amount of damage or loss." (Heng, 1996, p.12)

Definitions of Business Continuity

DEFINITION & SOURCE
"[...] ongoing process of risk assessment and management with the purpose of ensuring that the business can continue if risks materialize." (Msezane and McBride, 2002, p.350)
"[...] arrangement for emergency business and data center operations and recovery plan following a disaster." (Rosenthal and Sheiniuk, 1993, p.12; Chow, 2000, p.80)
"[...] interrupted provision of operations and services to customers, united with continuous accountability for key decisions." (Sun, 2004, p.1)

Definitions of Business Continuity Plan

DEFINITION & SOURCE
"[...] document used to assist an organization in recovering its business functions." (Hawkins, Yen *et al.*, 2000, p.222)
"[...] an institution's insurance policy assuring on-going operations, key data recovery and uninterrupted cash flow." (Luecke and Hoopingarner, 1993, p.30)
"[...] A plan for emergency response, backup operations and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation." (Oh, 2005, p.3)

Definitions of Business Continuity Planning

DEFINITION & SOURCE
"[...] focuses mainly on the disruption to the business." (Heng, 1996, p.11)
"Process of developing advanced arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change." (Beck, 2004, p.38)
"Planning which identifies the organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, whilst maintaining competitive advantage and value system integrity." (Elliott, Swartz *et al.*, 1999, p.48)
"[...] comprised of enterprise-level and end-to-end solutions, from design and planning to implementation and management, with the focus on being proactive." (Wilson, 2004)
"[...] determines how a company will keep functioning until its normal facilities are restored after a disruptive event." (Scalet, 2001)
" [...] an integrated set of procedures and resource information that firms can use to prevent or recover from a disaster which causes a disruption to business operations. " (Zsidisin, Melnyk *et al.*, 2004)
"BCP is a process to be governed by top management." (Grillo, 2003, p.12)
"[...] the overarching ability of the organization to continue business operations after disruption." (Hood, 2005, p.61)
"[...] the uninterrupted provision of operations and services to end-user customers." (AT&T, 2004, p.1)
"[...] involves developing a collection of procedures for the various business units that will ensure the continuance of critical business processes while the data center is recovering for disaster." (Botha and Von Solms, 2004, p.328)

Definitions of Disaster Recovery

DEFINITION & SOURCE
"[...] process of correcting the problem and getting the critical business functions back on-line." (Hawkins, Yen *et al.*, 2000, p.229)
"[...] restoration of computing and telecommunications services after an event has disrupted those services." (Scalet, 2001)
"[...] stand-alone set of emergency procedures and technology tools [...]."(Robinson, 2002, p.30)
"[...] restoration of normal operating procedures after a system failure." (Heikkinen and Sarkis, 1996, p.28)
"[...] restoration of specific assets, such as data networks, following an operational disruption." (AT&T, 2004, p.2)
"[...] – asset recovery and replacement, and the capacity to quickly and efficiently restore the process that makes your business happen." (Sun, 2004, p.1)

Definitions of Disaster Recovery Plan

DEFINITION & SOURCE
"[...] document designed to assist an organization in recovering from data losses and restoring data assets." (Hawkins, Yen *et al.*, 2000, p.222)
"[...] a predetermined set of instructions that describes the process of disaster recovery." (Hawkins, Yen *et al.*, 2000, p.229)
"[...] a written plan of action that enables a company to respond quickly and effectively to a disaster." (Bandyopadhyay and Schkade, 2000, p.74)
"[...] marshals a company's resources to deal prospectively with a variety of future adverse events that could disrupt business operations." (Weiner, 2001, p.23)
"[...] plan that is intended to reduce the disruption of an organization's essential business functions to an acceptable level of a disaster." (Cale and Dye, 1998, p.37)
"[...] a plan which allows installation to former business status when it suffers some kind of major damage or other disastrous event." (Chow, 2000, p.81)
"[...] a set of procedures that are used to ensure the recovery of relevant information within an affordable downtime when a disaster strikes." (Chow, 2000, p.81)
"[...] method by which a company identifies critical resources, determines how these resources are negatively impacted by a disaster, and develops a plan to minimize and recover from the negative impact of a disaster." (Carlson and Parker, 1998, p.11)

DEFINITION & SOURCE
"[...] a subset of the BCP. Its purpose is to recover essential IT systems, at least to some degree, in the event of a disruption or a disaster." (Oh, 2005, p.4)

Definitions of Disaster Recovery Planning

DEFINITION & SOURCE
"[...] a concern for computer security that provides alternatives for businesses facing contingency events that could be detrimental to the functions normally performed." (Chow, 2000, p.80)
"[...] planning how your business can recover from its former trading status if it should suffer some kind of major damage or other disastrous events." (Paradine, 1995, p.9)
"[...] the process of developing and maintaining an effective plan of how organizations will continue to operate in the event of interruptions of business functions." (Bandyopadhyay and Schkade, 2000, p.76)
"[...] focuses mainly on the recovery of the IT department and all related functions." (Botha and Von Solms, 2004, p.329)

Definitions of Critical Success Factors

DEFINITION & SOURCE
"Key areas of activity in which favorable results are necessary for a company to reach its goals." (DM Review, 2005)
"[...] things which must go right for the organization to achieve its mission." (Michaels, 2005)
"[...] a small number of key factors executives consider critical to the success of the enterprise, where successful performance will assure the success of the organization and attainment of its goals." (Vogl, 2005)

Definitions of Risk Assessment

DEFINITION & SOURCE
"[...] considers all possible threats to an IS such as natural disasters, hardware and/or software error, and human error." (Wong, Monaco *et al.*, 1994, p.29; Chow, 2000, p.81)
"[...] identifies corporate resources development, including infrastructure of the network." (Hawkins, Yen *et al.*, 2000, p.227)
"Process of identifying the risks to an organization, assessing the critical functions

DEFINITION & SOURCE
necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event." (DRI International, 2006a)
"[...] involves identifying the risks that the company is likely to face and then for each of the risks, assessing the likelihood of suffering any particular incident." (Williams, 2002, p.16)

Definitions of (Business) Impact Analysis

DEFINITION & SOURCE
"[...] includes an evaluation of the consequences of a disaster in each area of the business and assesses the maximum allowable IS downtime." (Wong, Monaco *et al.*, 1994, p.29; Chow, 2000, p.81)
"[...] identifies the mission-critical resources in the company [...]"(Hawkins, Yen *et al.*, 2000, p.227)
"Process designed to identify critical business functions and workflow, determine the qualitative and quantitative impacts of a disruption, and to prioritize and establish recovery time objectives." (Beck, 2004, p.38)
"[...] identifies critical functions the business must perform to stay in business; identifies risks to critical business functions and rates those risks according to probability of occurrence and impact on business; recommends avoidance, mitigation, or absorption of the risk, and identifies ways to avoid or mitigate the risk." (Cerullo and Cerullo, 2004, p.71)
"[...] means of systematically assessing the potential impacts resulting from various events of incidents that might cause existing facilities of systems to be unavailable." (Savage, 2002, p.256)

Definitions of Recovery Time Objective (RTO)

DEFINITION & SOURCE
"The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). [...] a determinant as to whether or not to implement the recovery strategies during a disaster situation." (DRIInternational, 2006a)
"[...] point in time after an interruption that business processes, functions and computer application data will be restored to ensure the viability of ongoing business operation." (Beck, 2004, p.40)
"[...] acceptable amount of time it would take for your organization to resume operations

DEFINITION & SOURCE
following a disaster." (XOSoft, 2004, p.1)

Definitions of Recovery Point Objective (RPO)

DEFINITION & SOURCE
"The point in time to which systems and data must be recovered after an outage. (e.g. end of previous day's processing). [...] a determinant of the amount of data that may need to be recreated after the systems or functions have been recovered." (DRIInternational, 2006a)
"[...] point in time, in accordance with the RTO, to which vital records, work-in-process or computer application data will be restored to ensure viability of ongoing business operations." (Beck, 2004, p.40)

Definitions of Contingency Planning

DEFINITION & SOURCE
"[...] process of developing and maintaining an effective written plan of how the organization will continue to operate in the event of interruption of business functions." (Andrews, 1990, p.29; (Bandyopadhyay and Schkade, 2000, p.76)
"Process of developing advance arrangements and procedures that enable an organization to respond to an event that could occur by chance or unforeseen circumstances." (DRIInternational, 2006a)
"[...] process of examining the possibilities of losing an IT system and formulating procedures and strategies to minimize the damage." (Nelson, 2000)
"[...] a plan that an organization will follow in the event of a disaster, outlining workplace requirements and a plan of action." (Scarinci, 2002, p.65)
"[...] process of examining an organization's critical functions, identifying the possible disaster scenarios and developing scenarios to address these concerns." (Botha and Von Solms, 2004, p.329)

APPENDIX III Most Prominent Financial US Regulations Since 9/11

Adapted from Archivas (2004), *Digital Archiving Strategies for Regulatory Compliance in Financial Services*, pp.2-3.

REGULATION	DESCRIPTION
SEC 17a-3 SEC 17a-4 ➢ 17a-4(b)(4) ➢ 17a-4(f) ➢ 17a-4(2)(i) ➢ 17a-4(2)(ii)(A) ➢ 17a-4(2)(ii)(C) ➢ 17a-4(2)(ii)(D) ➢ 17a-4(3)(i , ii)	While regulatory compliance in general is important for financial institutions, regulations governing securities trading are the most stringent and have set the bar for the rest of industry. A series of SEC rules referred to in section 17-4 deals with correspondence between the securities company and its customers. 17-4 specifies a firm's record keeping requirements with regards to purchase and sale documents, customer records, associated persons' records, customer complaint records and written supervisory procedures. 17a-3 specifies what types of documents have to be retained and for what period of time.
SEC 31a-1 and 204-2	Permits mutual fund companies and investment advisors to keep all of their records in an electronic format. Provides guidelines for archiving data.
Patriot Act	Makes businesses responsible for seeking, detecting, and reporting computer trespasses. Banks, in particular, are expected to identify, discover, gather, amass, investigate, and report on financial activity to a far greater degree and depth than ever.
Gramm-Leach-Bliley Act	Targeted at "financial institutions", including banks, credit unions, collection agencies, credit bureaus, check cashing companies, credit counseling organizations, brokers, tax planning and preparation companies, retailers that issue their own credit cards, auto dealers that lease and/or finance, companies that sell money orders and/or travelers checks, investment companies, investment advisors, and insurance companies. Provides limited privacy protections against the sale of private financial information on customers to third parties.
Sarbanes-Oxley Act (Section 802, Regulation S-X, Rule 2-06)	Affects all public companies. Mandates the retention of documents used for financial audits and reporting. Because of the stiff penalties, compliance with SOX mandates is a high priority for many financial services firms. Criminalizes spoilage and the intentional failure to preserve documents that are-or may one day be- required in litigation.
NASD Rule 3010 and 3110	Rules set by the National Association of Securities Dealers Inc. (NASD). Each firm must "supervise" their representatives' activity, including monitoring incoming and outgoing email. Each member shall retain correspondence of registered representatives relating to its investment banking or securities business.

APPENDIX IV Results of ProQuest® Search for Academic Material in the Business Continuity / Disaster Recovery Field

Search conducted on March 10, 2006.

Article Title ** / Publication Title *	**Information Management**		Systems		**Review**		**Journal**	
	Tot.	Aca. Rel.	Tot.	Aca. Rel.	Tot.	Aca. Rel.	Tot.	Aca. Rel.
Disaster Recovery	7	3	36	2	37	2	59	4
Contingency Plan*	1	1	19	0	7	0	48	3
Business Continuity	6	1	4	1	8	0	20	5
Business Recovery	0	0	2	0	2	0	9	0
Sub-Total	**14**	**5**	**61**	**3**	**54**	**2**	**136**	**12**
% academic relevancy	***36%***		***5%***		***4%***		***9%***	
TOTAL	***Academic = 22 articles*** ***All articles = 265 articles*** ***Percentage academic relevancy22 / 265 = 8.3%***							

LEGEND

Tot. = Total number of articles retrieved from the search

Aca. Rel. = Total number of academically relevant articles within a particular search.

* includes all results with the *Publication Title* keywords of "Information Management" "Systems", "Review" and "Journal" and includes articles that may be downloaded or read.

** criteria for acceptance are that it discussed issues pertaining to BC/DR, are academic (not practitioner) based and are non redundant (a particular article may be referenced in one or more publications).

Search criteria - ProQuest

Within the ProQuest® database search, the keywords "Disaster Recovery", "Contingency Plan*" (* is the wildcard that would include all derivatives containing such words as plan, plans, planning...), "Business Continuity" and "Business Recovery" are entered in the **Document Title** field. As well, each of the keywords were associated with the following keywords were associated with the **Publication Title** field:

"Information Management"
"Systems"
"Review"
"Journal"

The reason for the selection of the keywords within the Publication Title is because the top IT academic journals contain some combination of these words. For instance, the top 5 as mentioned in Peffers and Ya (2003) exhaustive study of 326 IS, allied disciplines and professional and managerial journals (2003) ranked accordingly:

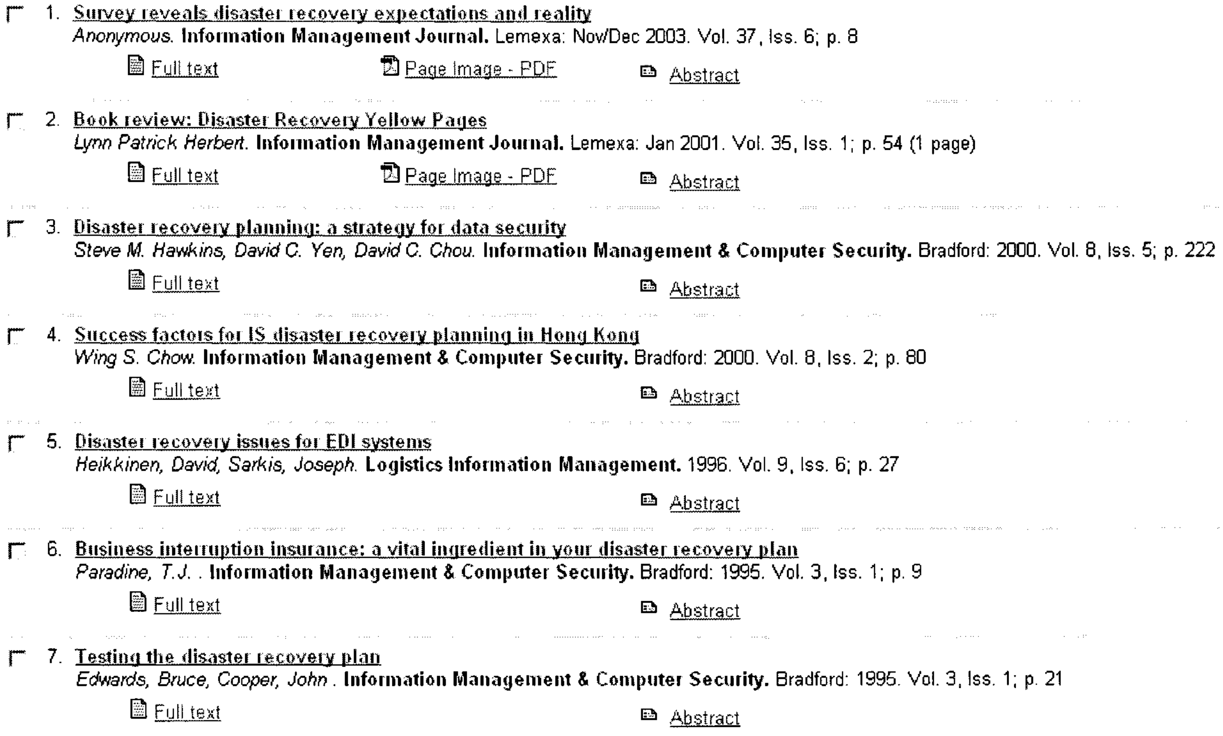
Weighted Ranking	Title	Total Weighted Ranking
1	MIS Quarterly (Management of Information Systems)	489.1
2	Information Systems Research	418.3
3	Journal of MIS (Management of Information Systems)	317.4
4	European Journal of Information Systems	303.8
5	Information and Management	303.8

Adapted from Peffers and Ya (2003), IS research journals, ranked by total weighted perceived value rating as outlets for information systems research, Table 3 Part A, .70.

As depicted above, all of the Publication Title keywords are somehow mentioned within each of the top 5 IS journal titles. In fact, of the top 50 described in the original table, 43 have some derivation of the above.

APPENDIX V Sample Query Screenshot of Academic Search Results in ProQuest®

LIBRARY:	ABI/Inform Global on ProQuest
ACCESS DATE:	March 11, 2006
ARTICLE TITLE	*Disaster Recovery*
PUBLICATION TITLE	*Information Management*
RESULTS:	*7 articles*



□ 1. Survey reveals disaster recovery expectations and reality
Anonymous. **Information Management Journal.** Lemexa: Nov/Dec 2003. Vol. 37, Iss. 6; p. 8
Full text Page Image - PDF Abstract

□ 2. Book review: Disaster Recovery Yellow Pages
Lynn Patrick Herbert. **Information Management Journal.** Lemexa: Jan 2001. Vol. 35, Iss. 1; p. 54 (1 page)
Full text Page Image - PDF Abstract

□ 3. Disaster recovery planning: a strategy for data security
Steve M. Hawkins, David C. Yen, David C. Chou. **Information Management & Computer Security.** Bradford: 2000. Vol. 8, Iss. 5; p. 222
Full text Abstract

□ 4. Success factors for IS disaster recovery planning in Hong Kong
Wing S. Chow. **Information Management & Computer Security.** Bradford: 2000. Vol. 8, Iss. 2; p. 80
Full text Abstract

□ 5. Disaster recovery issues for EDI systems
Heikkinen, David, Sarkis, Joseph. **Logistics Information Management.** 1996. Vol. 9, Iss. 6; p. 27
Full text Abstract

□ 6. Business interruption insurance: a vital ingredient in your disaster recovery plan
Paradine, T.J. . **Information Management & Computer Security.** Bradford: 1995. Vol. 3, Iss. 1; p. 9
Full text Abstract

□ 7. Testing the disaster recovery plan
Edwards, Bruce, Cooper, John . **Information Management & Computer Security.** Bradford: 1995. Vol. 3, Iss. 1; p. 21
Full text Abstract

APPENDIX VI Critical Success Factor (CSFs) Matrix

The matrix comprises the following elements:

- The first column indicates if the article is *Academic* (A) or *Non-Academic* (NA). Due to the lack of academic literature within the contingency planning field, practitioner articles were taken into consideration. Since empirical studies add greater credibility to research, a practitioner article needed to have at least 5 CSFs defined and explained to be included in the matrix.
- The matrix also indicates if the CSF in question within the article was stressed. A bolded **X** means that the CSF was explained using one of the following objectives/nouns:

Critical	Important	Vital
Imperative	Crucial	Essential
Top	Most	Key
Primary	Paramount	[a] Must

The articles within the matrix were classified chronologically. This was done to try and determine if article published after 9/11 were more practitioner or academically oriented.

LEGEND

CSF1	**TOP MGMT.COMMITMENT**
CSF2	**ADEQUATE FINANCIAL SUPPORT**
CSF3	**ALIGNMENT OF DRP OBJECTIVES WITH COMPANY GOALS**
CSF4	**ADOPTION OF PROJECT MANAGEMENT TECHNIQUES**
CSF5	**PRESENCE OF FORMAL RECOVERY PLANNING COMMITTEE**
CSF6	**PARTICIPATION OF REPRESENTATIVES FROM EACH DEPT.**
CSF7	**ENGAGEMENT OF EXTERNAL CONSULTANT**
CSF8	**RISK ASSESSMENT & IMPACT ANALYSIS**
CSF9	**IMPACT ANALYSIS**
CSF10	**DETERMINATION OF MAXIMUM ALLOWABLE IS DOWNTIME**
CSF11	**PRIORITIZATION OF IS APPLICATIONS**
CSF12	**OFF-SITE STORAGE OF BACKUP**
CSF13	**PRESENCE OF EMERGENCY RESPONSE PROCEDURES**
CSF14	**TRAINING OF RECOVERY PERSONNEL**
CSF15	**APPROPRIATE BACKUP SITE**
CSF16	**PERIODICAL TESTING OF DRP**
CSF17	**MAINTENANCE OF DRP**
CSF18	**INSURANCE COVERAGE FOR IS LOSS**
New CSFs	
CSF19	**EFFECTIVE COMMUNICATION**
CSF20	**SERVICE LEVEL AGREEMENTS (SLAs)**
CSF21	**BC/DR IMPLEMENTATION PLAN & TEMPLATES**

BEFORE EVENTS OF SEPTEMBER 11th, 2001 – CSFs 1 to 10

A/NA	AUTHORS	CSF1	CSF2	CSF3	CSF4	CSF5	CSF6	CSF7	CSF8	CSF9	CSF10
NA	Cerullo (1981)	X	X			X	X			X	
NA	Wuest (1988)	X					X				
NA	Andrews (1990)	X					X		X	X	
A	Rohde & Haskett (1990)	X	X	X					X		
NA	Haight & Byers (1991)	X					X		X	X	
NA	Luecke & Hoopingarner (1993)	X				X	X	X	X	X	
A	Rosenthal & Sheiniuk (1993)	X	X				X		X		
A	Vijayaraman & Ramakrishna (1993)										
A	Wong, Monaco *et al.* (1994)	X	X	X		X	X		X	X	X
A	Lee & Ross (1995)			X			X			X	X
NA	Moore (1995)						X	X			
NA	Smith (1995)								X	X	
NA	Paradine (1995)								X	X	
NA	Heng (1996)	X			X				X	X	X
A	Heikkinen & Sarkis (1996)								X		X
NA	Karakasidis (1997)	X	X		X		X		X	X	

A/N A	AUTHORS	CSF1	CSF2	CSF3	CSF4	CSF5	CSF6	CSF7	CSF8	CSF9	CSF10
NA	**Jacobs & Weiner (1997)**	X	X		X	X	X	X			
A	**Carlson & Parker (1998)**	X					X				
NA	**Payne (1999)**					X	X				
A	**Paton (1999)**			X			X		X	X	
A	**Jordan (1999)**	X					X	X	X		
A	**Nelson (1999)**	X		X				X			
A	**Elliott, Swartz *et al.* (1999)**	X		X			X				
A	**Chow (2000)**	X	X	X	X	X	X	X	X	X	X
A	**Hawkins *et al.* (2000)**	X			X	X	X	X	X	X	
A	**Bandyopadhyay& Schkade (2000)**	X	X					X			
A	**Iyer & Bandyopadhyay (2000)**	X	X	X			X		X	X	X
NA	**Clifton (2000)**	X			X		X		X	X	

AFTER EVENTS OF SEPTEMBER 11th , 2001 – CSFs 1 to 10

A/N A	AUTHORS	CSF1	CSF2	CSF3	CSF4	CSF5	CSF6	CSF7	CSF8	CSF9	CSF10
NA	Weiner (2001)								X	X	
A	Laye & Torre-Enciso (2001)	X					X		X		
NA	Savage (2002)	X					X	X	X	X	
A	Msezane & McBride (2002)	X					X		X		
NA	Carvajal-Vion & Garcia								X	X	
A	Grillo (2003)	X	X	X					X	X	
NA	Bielski (2003)	X	X				X		X	X	
NA	Lim (2003)	X					X				
A	Pitt & Goyal (2004)	X		X		X	X	X	X	X	X
NA	AT&T White Paper (2004)	X				X	X	X			
A	Quirchmayr (2004)							X			X
A	Zsidisin, Ragatz *et al.* (2004)										
A	Cerullo & Cerullo (2004)	X	X				X		X	X	
A	Castillo (2004)						X		X	X	
NA	Beck (2004)	X	X	X	X		X		X	X	X
NA	Hood (2005)										

BEFORE EVENTS OF SEPTEMBER 11th, 2001 – CSFs 11 to 21

A/N A	AUTHORS	CSF 11	CSF 12	CSF 13	CSF 14	CSF 15	CSF 16	CSF 17	CSF 18	*CSF 19*	*CSF 20*	*CSF 21*
NA	Cerullo (1981)	X	X		X	X	X					
NA	Wuest (1988)	X	X			X	X	X				
NA	Andrews (1990)	X				X	X				X	
A	Rohde & Haskett (1990)	X	X			X	X					
NA	Haight & Byers (1991)	X	X		X	X	X					
NA	Luecke & Hoopingarner (1993)	X	X						X			X
A	Rosenthal & Sheiniuk (1993)		X		X	X	X					
A	Vijayaraman & Ramakrishna (1993)					X			X	X		
A	Wong, Monaco *et al.* (1994)	X		X	X	X	X	X	X	X	X	
A	Lee & Ross (1995)	X	X		X	X	X	X	X			
NA	Moore (1995)			X		X			X			
NA	Smith (1995)		X			X	X			X		
NA	Paradine (1995)		X				X	X	X			
NA	Heng (1996)			X	X	X	X	X				
A	Heikkinen & Sarkis (1996)		X	X			X	X				
NA	Karakasidis (1997)	X				X	X	X		X	X	X

A/NA	AUTHORS	CSF 11	CSF 12	CSF 13	CSF 14	CSF 15	CSF 16	CSF 17	CSF 18	CSF 19	CSF 20	CSF 21
NA	**Jacobs & Weiner (1997)**	X	X		X	X		X	X		X	
A	**Carlson & Parker (1998)**		X			X					X	
NA	**Payne (1999)**											
A	**Paton (1999)**			X	X							
A	**Jordan (1999)**				X							
A	**Nelson (1999)**						X					
A	**Elliott, Swartz *et al.* (1999)**											
A	**Chow (2000)**	X	X	X	X	X	X	X	X			
A	**Hawkins, Yen *et al.* (2000)**	X	X		X	X	X	X	X		X	
A	**Bandyopadyay& Schkade (2000)**											
A	**Iyer & Bandyopadhyay (2000)**	X	X	X	X	X	X	X	X		X	
NA	**Clifton (2000)**			X	X	X		X				X

AFTER EVENTS OF SEPTEMBER 11th , 2001 – CSFs 11 to 21

A/N A	AUTHORS	CSF 11	CSF 12	CSF 13	CSF 14	CSF 15	CSF 16	CSF 17	CSF 18	CSF 19	CSF 20	CSF 21
NA	Weiner (2001)		X	X					X			X
A	Laye & Torre-Enciso				X	X	X					
NA	Savage (2002)		X	X	X	X	X	X	X	X	X	X
A	Msezane & McBride (2002)			X		X		X				
NA	Carvajal-Vion & Garcia (2003)						X	X			X	
A	Grillo (2003)	X	X			X	X	X				X
NA	Bielski (2003)	X					X	X		X		
NA	Lim (2003)	X			X							
A	Pitt & Goyal (2004)	X		X	X		X	X		X		
NA	AT&T White Paper (2004)				X		X	X		X		
A	Quirchmayr (2004)	X					X					
A	Zsidisin, Ragatz et. al (2004)				X			X				
A	Cerullo & Cerullo (2004)				X		X				X	
A	Castillo (2004)					X	X	X				
NA	Beck (2004)		X	X	X		X	X		X		
NA	Hood (2005)	X			X		X	X			X	

APPENDIX VII Top Management Commitment Passages

PASSAGE	AUTHOR
“Previous research in crisis strategic management suggests that top management support is a critical prerequisite to development of crisis plans.”	(Nelson 2000, p.1266).
“Senior management tracking [...] ensures organizational commitment [...].”	(Cerullo and Cerullo, 2004, p.71).
“CEO involvement was also held to be the key in rallying support for the DRP process.”	(Elliott, Swartz *et al.,* 1999, p.56)
“Seeking management commitment is the most critical area of the project planning process”.	(Heng, 1996, p.12)
“Top management commitment is vital to the success of any disaster recovery plan”.	(Wong, Monaco *et al.*, 1994, p.29)
“Thus, strong management commitment is an essential ingredient for a successful DRP program.”	(Bandyopadhyay and Schkade, 2000, p.79)

APPENDIX VIII Statistics on how Senior Management Views Business Continuity Planning

- Only four in 10 company officers who have responsibility for BCP at companies with annual revenues of $25 million or more (42%) say BC has always been a priority for their company, while 25% say it has only become a priority in recent years due to security and terrorist threats.

- Twenty-six percent say BCP is important, but not a high priority, while 5% admit it is not important for their company.

- Companies with more than 500 employees place only slightly more importance on BC than smaller companies (74% vs. 65%).

- Not surprisingly, far more companies that have a plan say BC has always been a priority (52%) than companies without a plan (15%).

- BCP in *not* a higher priority at companies that suffered a business disaster (69%) than at those which haven't (67%). Companies in finance, insurance and real estate (57%) are the most likely to have always made BC a priority, while those in manufacturing are the most likely to say it is not a priority (40%).

- Of the three in 10 company officers who have responsibility for BCP who say BC is not a high priority, the most common reasons they cite for its lack of importance are other issues taking priority (68%), they consider the systems in place sufficient (61%), the low probability a major disaster will hit their company (58%), expense (39%) and unfamiliarity at the company with the process required to ensure BC (27%).

(as referenced in Anonymous, 2004b, p.5)

APPENDIX IX Professional Practices for Business Continuity Professionals

DISASTER RECOVERY INFORMATION INTERNATIONAL (DRII)

1. Project Initiation and Management

Establish the need for a Business Continuity Management (BCM) Process or Function, including resilience strategies, recovery objectives, business continuity and crisis management plans and including obtaining management support and organizing and managing the formulation of the function or process either in collaboration with, or as a key component of, an integrated risk management initiative.

2. Risk Evaluation and Control

Determine the events and external surroundings that can adversely affect the organization and its resources (facilities, technologies, etc.) with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.

3. Business Impact Analysis

Identify the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts. Identify time-critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set.

4. Developing Business Continuity Management Strategies

Determine and guide the selection of possible business operating strategies for continuation of business within the recovery point objective and recovery time objective, while maintaining the organization's critical functions.

5. Emergency Response and Operations

Develop and implement procedures for response and stabilizing the situation following an incident or event, including establishing and managing an Emergency Operations Center to be used as a command center during the emergency.

6. Developing and Implementing Business Continuity and Crisis Management Plans

Design, develop, and implement Business Continuity and Crisis Management Plans that provide continuity within the recovery time and recovery point objectives.

7. Awareness and Training Programs

Prepare a program to create and maintain corporate awareness and enhance the skills required to develop and implement the Business Continuity Management Program or process and its supporting activities.

8. Maintaining and Exercising Plans

Pre-plan and coordinate plan exercises, and evaluate and document plan exercise results. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the organization's strategic direction. Verify that the Plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner.

9. Crisis Communications

Develop, coordinate, evaluate, and exercise plans to communicate with internal stakeholders (employees, corporate management, etc.), external stakeholders (customers, shareholders, vendors, suppliers, etc.) and the media (print, radio, television, Internet, etc.).

10. Coordination with External Agencies

Establish applicable procedures and policies for coordinating continuity and restoration activities with external agencies (local, state, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes or regulations.

Taken from DRI International web site (DRI International 2006b)

BUSINESS CONTINUITY INSTITUTE (BCI)

1. Initiation and Management

Establish the need for a Business Continuity Management (BCM) Process or Function, including resilience strategies, recovery objectives, business continuity and crisis management plans and including obtaining management support and organising and managing the formulation of the function or process either in collaboration with, or as a key component of, an integrated risk management initiative.

2. Business Impact Analysis

Identify the impacts resulting from disruptions and disaster scenarios that can affect the organisation and techniques that can be used to quantify and qualify such impacts. Identify time-critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set.

3. Risk Evaluation and Control

Determine the events and external surroundings that can adversely affect the organisation and its resources (facilities, technologies, etc.) with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimise the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.

4. Developing Business Continuity Management Strategies

Determine and guide the selection of possible business operating strategies for continuation of business within the recovery point objective and recovery time objective, while maintaining the organisation's critical functions.

5. Emergency Response and Operations

Develop and implement procedures for response and stabilising the situation following an incident or event, including establishing and managing an Emergency Operations Centre to be used as a command centre during the emergency.

6. Developing and Implementing Business Continuity and Crisis Management Plans

Design, develop, and implement Business Continuity and Crisis Management Plans that provide continuity within the recovery time and recovery point objectives.

7. Awareness and Training Programmes

Prepare a programme to create and maintain corporate awareness and enhance the skills required to develop and implement the Business Continuity Management Programme or process and its supporting activities.

8.Maintaining and Exercising Business Continuity and Crisis Managements Plans

Pre-plan and co-ordinate plan exercises, and evaluate and document plan exercise results. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the organisation's strategic direction. Verify that the Plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner.

9. Crisis Communications

Develop, co-ordinate, evaluate, and exercise plans to communicate with internal stakeholders (employees, corporate management, etc.), external stakeholders (customers, shareholders, vendors, suppliers, etc.) and the media (print, radio, television, Internet, etc.).

10. Co-ordination with External Agencies

Establish applicable procedures and policies for co-ordinating continuity and restoration activities with external agencies (local, state, national, emergency responders defence, etc.) while ensuring compliance with applicable statutes or regulations.

APPENDIX X Backup Recovery Strategy Options

TYPE	DESCRIPTION	ADVANTAGES	DISADVANTAGES	AUTHOR(S)
Relocate & Restore (Real Estate Broker strategy)	A suitable location is identified and all hardware, software and systems are set up and configured after an emergency has been declared	• No cost until disaster declared	• Only viable for non-critical systems	(Savage, 2002)
Reciprocal Agreement (Buddy Site)	A corporate bilateral agreement whereby each organization agrees to provide the other the use of its DR facilities in the event of a disaster.	• Very inexpensive • Can be established early if services provided by both organizations similar • Less training intensive	• Only viable if one of the companies is not affected • Other company might not have capacity for the other	(Haight and Byers, 1991; Wong, Monaco *et al.*, 1994; Savage, 2002)
Service Bureaus	Private company which makes itself available to take over an organization's DR activities should a disaster occur.	• Inexpensive • No need to move employees/equipment	• Difficult transition from company to bureau • Limited availability	(Haight and Byers, 1991; Wong, Monaco *et al.*, 1994)
Warm (Cold) Site	A shell that is ready to be installed with DR equipment in the event of a disaster. May also be mobile.	• Less expensive that Hot Site • Lower declaration fee	• Time consuming until vendor delivers equipment • Possible installation issues	(Haight and Byers, 1991; Wong, Monaco *et al.*, 1994; Iyer and Bandyopadhyay, 2000; Savage, 2002)
Hot Site	Commercially (publicly) or corporately (privately) maintained Disaster Recovery (DR) center which has most or all of the same equipment as the primary center.	• Very fast means to continue activities • Can run almost any application • Short-term solution	• Very expensive • Disaster decalartion fee • Limited space • Specific equipment may not be available	(Haight and Byers, 1991; Wong, Monaco *et al.*, 1994; Iyer and Bandyopadhyay, 2000; Savage, 2002)
Fully Mirrored Recovery Site (Internal Site)	A fully redundant, duplicate recovery site with instantaneous switching between backup and live sites	• Automatic • Instantaneous • Low risks	• Most expensive	(Iyer and Bandyopadhyay, 2000; Savage, 2002)

APPENDIX XI Off-site Storage Factors

- **Location**: Ideally situated far enough from the company so that the probability of being affected by the same disaster is greatly reduced, but not too distant as to be inaccessible by simple means of transportation (Rohde and Haskett, 1990; Lee and Ross, 1995).

- **Frequency** of data/equipment backups: needs to be determined from the outset. Backups performed based upon factors as criticality, use and retention of data. A backup schedule should be discussed and agreed upon by all parties and inserted into the BC/DR plan.

- **Forms** of data backup are also of issue. Information is mostly backed up through technological means as tape, disk, microfiche, CD-ROM and DVD (Rohde and Haskett, 1990). However, physical forms such as photocopies of printed material also need to be stored off-site. Of note are the main means of transferring data from the parent site (corporate) to the backup location: these can be physical (safes, trucks, cars, vaults…) or logical (network, Internet…).

- **Architectures** for protecting critical data from interruptions are likewise important to consider. Three major approaches defined by Rosenthal & Sheiniuk (1993) include commercial data centers, multiple in-house data centers and distribution of processing to multiple user locations. Selecting the appropriate architecture depends upon the criticality of information, level of tolerance and cost.

- **Physical risk exposures** are amongst the most difficult to identify as attested by Weiner (2001). Proximity to hazardous materials, industry risk factors and physical location are examples of such exposures that need proper mitigation. Identifying, analyzing and understanding such threats "are well worth the time and money if disaster occurs" (p.25).

APPENDIX XII Recovery Backup Methods & Technologies

TYPE	DESCRIPTION	ADVANTAGES	DISAVANTAGES	AUTHOR(S)
1. Image Backup	[…] process that can completely back-up a partition or entire physical hard drive on a low-level, bit-by-bit basis	• Fast • Simple	• Maintenance intensive	(Edwards, 2003, p.18; Price, 2002, p.19)
2. Data Replication	[…] involves periodically copying a volume's data onto a secondary storage device which can be located at any distance from the original in a disk-to-disk method 3 Types (methods) of replication → Data mirroring → Tape-based backup → Continuous backup	• Distance independent • Continuous process • Very fast • Flexible		(Chalaka, 2003, p.36; Rapaport, 2004, p.30)
2.1 Data Mirroring	[…] involves the user of a "shadow" disk that is updated in parallel with the primary disk, providing a real-time copy of the primary disk. 3 technologies/solutions to data mirroring ➔ Synchronous ➔ Asynchronous ➔ Snapshot-enhanced (mix of above)	(Please refer to the synchronous and asynchronous sections)	(Please refer to the synchronous and asynchronous sections)	(Chalaka, 2003, p.36)
2.1.1 Synchronous Mirroring/ Replication	Each time an application attempts to write data to disk, the transaction is sent to both the local and remote storage devices in parallel. It is not until both devices have committed the write to disk that the system acknowledges a complete transaction.	• Maximum data protection (no data is lost in transition)	• Performance degradation at primary site • Higher bandwidth (reduced network throughput) • More equipment • More costly • Less distance	(Rodriguez, 1997, p.47; Chudnow, 2001, p.52; Nahum; 2003, p.36; Chalaka, 2003, p.46; Rapaport, 2004, p.31; Burgener, 2004, p.24)

2.1.2 Asynchronous Mirroring/ Replication	Each transaction is acknowledged as soon as the local storage device completes the request, even if the remote system has not received and/or processed the request. 2 Types of asynchronous mirroring → Server-based mirroring → Storage-based mirroring → Appliance-based mirroring	• Little performance degradation at primary site • Minimal bandwidth • Less equipment • Less costly • Greater distance	• Data may be lost during transmission	(Rodriguez, 1997, p.47; Chudnow, 2001, p.52; Nahum; 2003, p.36; Chalaka, 2003, p.46; Rapaport, 2004, p.31; Burgener, 2004, p.24)
2.1.2.1 Server-based mirroring	[…] uses the hosts CPU to manage data replication	• DAS or NAS support • Heterogeneous storage support	• No support for heterogeneous servers • Vendor lock-in with volume manager / file system • Appl. performance / scalability limits • Increased work for storage mediums	(Nahum, 2003, p.37; Burgener, 2004, p.24)
2.1.2.2 Storage-based mirroring	[…] uses dedicated mirroring controller to manage data replication	• Heterogeneous server support	• No support for heterogeneous storage • Increased burden on storage controller • Vendor lock-in at any level / Must be secure • Very costly	(Nahum, 2003, p.37; Burgener, 2004, p.24)
2.1.2.3 Appliance-based mirroring	[…] uses clustering to manage data replication	• Heterogeneous server and storage support	• SAN support only • Drives additional hardware purchases	(Burgener, 2004, p.24)

			(e.g.: clustering appliances) • Appliance can be performance bottleneck	
2.1.3 Snapshot Enhanced Mirroring	Technology that combines platform-independent, any-to-any, asynchronous mirroring with low-capacity, instant point-in-time snapshots to ensure data integrity between sites while enabling rapid recovery after disaster	• Can utilize same snapshots for other purposes • Optimal performance • Limited bandwidth • Consistent copies of data on both sides • Less buffers	•	(Nahum, 2003, p.36)
2.2 Tape-based backup	[…] solution that stores a point-in-time copy of the operational data as inexpensive media that can be moved to a remote location and safely stored	•	• Backup window problems related to downtime • Data loss issues • Tape media data integrity issues • Wear out more quickly	(Burgener, 2004, p.24)
2.3 Continuous backup	Ensures that all data operations are captured and recorded to a journal at all times	• Highest data integrity • Highest recovery speed • Great amount of data backed up • Instantaneous recovery	• Costly	(Rapaport, 2004, p.31)
3. Disk-to-disk backup	Practice of protecting data using hard disk as a primary backup medium	• Speedier backups • Speedier restore • Cost effective	• Could propagate a virus	(Ferelli, 2002)

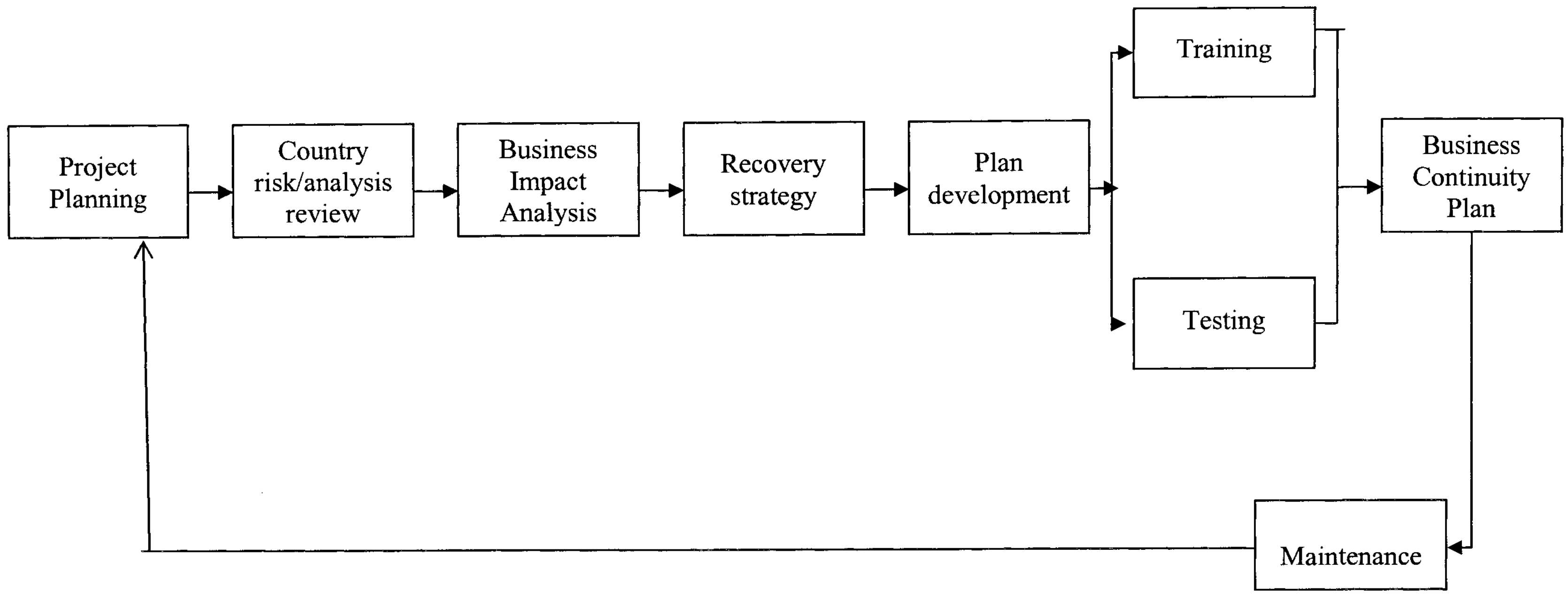
APPENDIX XIII Types & Classes of Recovery Tests

TYPE	DESCRIPTION	KEY POINTS	AUTHOR(S)
Simulation testing	Process of executing a sequence of steps in the BC/DR plan as though a real disaster had occurred.	• Most feasible approach for testing decision-making aspects of disaster reaction activities. • Mostly paper and pencil simulations. • Very successful since force personnel o learn BC/DR plan while working together, and finding flaws and inconsistencies in procedures.	(Wong, Monaco *et al*,. 1994; Rosenthal and Sheiniuk, 1993; Savage 2002)
Walkthrough testing	Process of identifying all of the steps and tasks necessary to successfully complete a test.	• Concerned with actually trying the contingency plan	(Wong, Monaco *et al.*, 1994; Cerullo, 1981; Savage, 2002)
Think-through testing Unit testing	Verbal undertaking of the contingency plan Process of testing individual prices of the overall contingency plan.	• Similar to walkthrough testing but done in a verbal manner • Part of the Module class of testing	(Cerullo, 1981) (Wong, Monaco *et al.*, 1994)
Parallel testing	Duplications of regular processing for a particular time frame.	•	(Wong, Monaco *et al.*, 1994),
Mock testing	Simulates actual disaster conditions by interrupting service and involving key users in the actual recovery process.	• Similar to Simulation testing but in a live environment.	(Wong, Monaco *et al.*, 1994),
Operational testing (Demonstrations)	Actually performing critical computer and non-computer tasks using real backup resources and facilities	• Actual, live testing of the whole recovery cycle of the documented plan. • Bottlenecks and loopholes should be discovered	(Rosenthal and Sheiniuk, 1993; Cerullo, 1981)
Application testing	Process of testing all of the critical applications.	• Part of the Full class of testing	(Wong, Monaco *et al.*, 1994)

CLASS	DESCRIPTION	KEY POINTS	AUTHOR(S)
Hypothetical	Testing that verifies the existence of all necessary procedures and actions specified within the recovery plan and consequently proving the theory behind these procedures	• Theoretical check that should be conducted bi-yearly • Brief exercise lasting approximately 2 hours • TYPES: Simulation, Think through	(Edwards and Cooper, 1995)
Component	Designed to very the detail and accuracy of individual procedures within the recovery plan and can be used when no additional system can be made available for extended periods	• Enables the ability to test specific functions without compromising production. • TYPES: Walkthrough	(Edwards and Cooper, 1995)
Module	Verify the validity and functionality of the recovery procedures when multiple components are combined.	• If you are able to test all modules, then you can be confident that the business will survive a major computer centre disaster. • TYPES: Unit, Parallel	(Edwards and Cooper, 1995)
Full	Verifies that each component within every module is workable and satisfies the strategy and timeframe requirements detail in the recovery plan.	• Verifies the interdependencies of various modules • TYPES: Mock, Operational, Application	(Edwards and Cooper, 1995)

APPENDIX XIV Standard Chartered Bank (SCB) Business Continuity Planning Methodology

(as defined by (Heng, 1996, p.12))



APPENDIX XV Karakasidis' 11-Step Methodology

1. Obtain top management approval and support.
2. Establish a business continuity planning (BCP) committee.
3. Perform business impact analysis.
4. Evaluate critical needs and prioritize business requirements.
5. Determine the business continuity strategy and associated recovery processes.
6. Prepare business continuity strategy and its implementation plan for executive management approval.
7. Prepare business recovery plan templates and utilities, finalize data collection and organize/develop the business continuity procedures.
8. Develop the testing criteria and procedures.
9. Test the business recovery process and evaluate test results.
10. Develop/review service level agreements (SLAs).
11. Update/revise the business recovery procedures and template

(as described in Karakasidis, 1997, p.72).

APPENDIX XVI Interview Questionnaire with Cover Page Letter

John Molson
School of Business
Concordia University

John Molson School of Business
Concordia University
1550 de Maisonneuve Blvd. West
Montreal, PQ, H3G 1M8, Canada
Phone: 514.848.2424
Fax: 514.848.2824

RESEARCH INTERVIEW

Conducted with: ______________________________

Organization: ______________________________

Title: ______________________________

Date: ______________________________

Time: From __________ to ______________

Location: ______________________________

This interview is conducted with the sole consent of the participant. At any time, the latter may refuse to answer a particular question and is free to withdraw from the process at any time.

Confidentiality of the results will be ensured and anonymity will be ensured upon publication as per the Research Protocol duly signed.

Interviews will be audio-recorded and transcribed to hardcopy thereafter. This is done to ensure a reliable, thorough analysis and the ability to measure validity of the issues upon transcription.

The participant will have the opportunity to review and comment on the hardcopy of the interview prior to analysis.

The final results of this research should provide the basis for academic and business publications.

QUESTION #1

How would you describe Business Continuity and Disaster Recovery (BC/DR) for your firm?

(Leading question)
On a scale of 1 – 7, how important is the issue of BC/DR?

____

____

____

QUESTION #2

What were the driving forces that led to the adoption of a BC/DR program for your organization?

(Leading question)
Were there any forces that stood out as being more important?

____

____

____

QUESTION #3

What are the current procedures and policies in place since the initial implementation of the BC/DR program?

____

____

____

How have the events of 9/11 affected your BC/DR program with respect to these procedures and policies?

____

____

QUESTION #4

How frequently is BC/DR program discussed as a strategic issue at the corporate level? How many people are directly involved in the BC/DR program in the organization?

____

____

____

QUESTION #5

What are the main benefits of BC/DR for your company?

____

____

____

What are the some of the drawbacks?

____

____

____

QUESTION #6

What are the main factors that you attribute to a recovery strategy being deemed successful?

____

____

____

APPENDIX XVII **Interview Consent Form**

John Molson
School of Business
Concordia University

John Molson School of Business
Concordia University
1550 de Maisonneuve Blvd. West
Montreal, PQ, H3G 1M8, Canada
Phone: 514.848.2424
Fax: 514.848.2824

CONSENT FORM TO PARTICIPATE IN RESEARCH

This is to state that I agree to participate in a program of research being conducted by **Mr. Michael Barbara**, a Masters in Science of Administration candidate from Concordia University and supervised by **Dr. Kevin Laframboise**, Assistant Professor at Concordia. Mr. Barbara can be reached at his office (514-847-6043), on his cellular (514-608-3501) or via e-mail at mbarbara@ogilvyrenault.com. Dr. Laframboise can likewise be contacted at his office (514-848-2424 ext. 2978) or by e-mail at lafrak@jmsb.concordia.ca

A. PURPOSE

The purpose of this research is to determine the main success factors of an effective business continuity / disaster recovery strategy and verify if these have changed since the events of September 11th, 2001. A framework of such factors will be proposed that may aid practitioners and academics alike.

B. PROCEDURES

The interview will be guided by the condition and procedures of the attached *Research Protocol.*

C. CONDITIONS OF PARTICIPATION

- I understand that I am free to withdraw my consent and discontinue my participation at anytime without negative consequences.
- I understand that my participation in this study is CONFIDENTIAL (i.e., the researchers will know, but will not disclose my identity) and that the data from this study will be anonymous and may be published.

I HAVE STUDIED THE ATTACHED RESEARCH PROTOCOL AND UNDERSTAND THIS AGREEMENT. I FREELY CONSENT AND VOLUNTARILY AGREE TO PARTICIPATE IN THIS STUDY.

NAME (please print) ____
SIGNATURE ____

If at any time you have questions about your rights as a research participant, please contact Adela Reid, Research Ethics and Compliance Officer, Concordia University, at (514) 848-7481 or by email at areid@alcor.concordia.ca.

APPENDIX XVIII Interview Research Protocol

John Molson School of Business
Concordia University
1550 de Maisonneuve Blvd. West
Montreal, PQ, H3G 1M8, Canada
Phone: 514.848.2424
Fax: 514.848.2824

RESEARCH PROTOCOL - INTERVIEWS

Objective

This protocol pertains to a research project aimed at determining what constitutes an effective business continuity / disaster recovery program within corporations. The ultimate objective is to establish a framework that may aid practitioners and academics alike in determining such strategies.

This project has been fully designed and conducted by **Michael Barbara**, an M.Sc.A. candidate at Concordia University. The thesis is supervised by **Kevin Laframboise, Ph.D.**. The other members of the committee are Anne-Marie Croteau, Ph.D and El-Sayed Abou-Zeid, Ph.D.

Participation

1. Individual participants asked to contribute to this study represent senior-level employees who have been involved in some capacity with the implementation of a business continuity / disaster recovery program. As senior employees, whether coordinators, managers or directors, their experience and knowledge on the subject matter is considered essential to a proper appreciation of issues of business continuity / disaster recovery.
2. This research intends to determine what are the main success factors that drive an effective business continuity / disaster recovery program in a post September 11th, 2001 world. Through participation, you will have a greater appreciation for the factors that are considered critical.

Conditions

A research interview protocol that is agreed to by the participant not only protects the participant and the researcher, but it also reduces variability of method. The following conditions shall be adhered throughout the interview process:

1. Participation on the part of the interviewee is entirely voluntary and the latter may withdraw participation at any time prior to the analysis of the data.
2. Interviews will be audio-recorded and transcribed to hardcopy thereafter. This is done to ensure a reliable, thorough analysis and the ability to measure validity of the issues upon transcription.
3. The participant will have the opportunity to review and comment on the hardcopy of the interview prior to analysis.

4. The final results of this research should provide the basis for academic and business publications.
5. Confidentiality of the participant and of the corporation's name are ensured. As well, in no way shall the participant be prejudiced by the information provided in the interview.
6. The data provided will be treated anonymously upon publication.

Procedure

The interview will be guided by the following procedure:

1. The interview will occur at the offices of the participating interviewee at a time convenient to him/her.

2 The interview should take between 30 to 45 minutes.

3. A report of the results of this study will be made available.

Sample Questions

The questions of the interviews would be similar to:

1. How would you describe business continuity / disaster recovery for your firm? How important is the issue of business continuity / disaster recovery?
2. What are the current procedures and policies in place? How have the events of 9/11 affected your business continuity / disaster recovery program with respect to the latter? How would you rank such procedures/policies?
3. How frequently is business continuity / disaster recovery discussed as a strategic issue at the corporate level? How many people are directly involved in business continuity / disaster recovery in the organization?
4. What are the main benefits of business continuity / disaster recovery for your company? What are the some of the drawbacks?
5. What are the main driving forces for business continuity / disaster recovery in your firm? How were these forces implemented within your corporation?

Appreciation

The members of this research team are indeed indebted to the participants who have agreed to partake in this project. On an individual basis, such contributions serve to help anyone to review personal views and thoughts on the issues. Collectively speaking, contributions help advance the science and reality of business administration. On behalf of the project team, we thank you for the opportunity.

Michael Barbara, M.Sc. Candidate	Kevin Laframboise, Ph.D.
Concordia University	Concordia University
Decision Sciences & M.I.S. Department	Decision Sciences & M.I.S.
Department	

If at any time you have questions about your rights as a research participant, please contact Adela Reid, Research Ethics and Compliance Officer, Concordia University, at (514) 848-7481 or by email at areid@alcor.concordia.ca.

APPENDIX XIX Variable/Critical Success Factor Cross-Referencing Schema

VARIABLE/CONCEPT IN INTERVIEW	RELATED CSF
Management […] supported Management […] approved and sanctioned Business Sponsor Executive Buy-In	Top Management Support (CSF1)
[…] set adequate financial budget	Adequate Financial Support (CSF2)
[…] incorporate defined objectives and targets that must be met […] […] IT coordinates recovery effort with Business Units (BUs) […] DR is part of the overall corporate objectives	Alignment of BCP/DRP Objectives with Company Goals (CSF3)
IT Council Committee of PC owners	Presence of Formal Recovery Planning Committee (CSF5)
[…] roles of all people involved […] allows staff to become familiar with all aspects of DR […] […] all resources are exposed to different scenarios	Participation of Representatives from each Department (CSF6)
3rd Party Provider Outsourcing to consultant	Engagement of External Consultant (CSF7)
Assessment of the impacts […]	Risk Assessment (CSF8)

Needs Analysis BIA	Business Impact Analysis (CSF9)
Prioritize elements Determine criticality Critical requirements and classification […] classify all degree of risk and uncertainty […] critical systems are evaluated and classified	Prioritization of IS applications (CSF11)
Communication Plan to educate Education & Awareness BC/DR promotion	Training (CSF13)
Negotiate External Support to have proper recovery Alternate Site Bunker	Appropriate Backup Site (CSF15)
[Keeping the DR plan] up-to-date Well-documented and well-maintained Creation of Post-mortem report Complete review of […] DR plan	Maintenance of BCP/DRP (CSF17)
[…] aid in the implementation of …	BC/DR Implementation Plan (CSF21)

APPENDIX XX Survey Questionnaire with Cover Page Letter

John Molson School of Business
Concordia University
1550 de Maisonneuve Blvd. West
Montreal, PQ, H3G 1M8, Canada
Phone: 514.848.2424
Fax: 514.848.2824

BUSINESS CONTINUITY/DISASTER RECOVERY (BC/DR) SURVEY

Thank you for participating in this Business Continuity/Disaster Recovery (BC/DR) study headed by **Mr. Michael Barbara**, Master's of Science in Administration candidate at Concordia University and supervised by **Dr. Kevin Laframboise**, Assistant Professor, Concordia University.

This study aims to shed light on the critical success factors of an effective BC/DR program and to confirm if these factors have changed from earlier research. As a subset of Business Continuity, we believe that the field of Disaster Recovery has been altered by the events of September 11th, 2001 and have consequently changed the way businesses view what they deem is necessary for a successful recovery.

The study is targeted to practitioners in the field who have an active role in defining, implementing or approving BC/DR policies, procedures and/or purchases. It is therefore assumed that a BC/DR program is in place or is being implemented at your location/organization.

This questionnaire contains **24** questions and should take approximately 20 minutes to complete. We request that the results be submitted no later than **Friday, December 16th, 2005**. Please complete the study in its entirety and focus on your own plant's/service's location in your responses.

You are free to withdraw and discontinue participation at anytime without negative consequences and it is understood that your participation in this study will be treated CONFIDENTIALLY. At the end of the research, the results (anonymously treated) will be made available to those who request it.

Should you have any specific questions regarding any part of this project, please feel free to contact Michael Barbara, M.Sc. candidate, Concordia University at (450) 687-3255 or at m_barbar@jmsb.concordia.ca

We wish to thank you for your contribution to this research. Your participation is invaluable.

If at any time you have questions about your rights as a research participant, please contact Adela Reid, Research Ethics and Compliance Officer, Concordia University, at (514) 848-7481 or by email at areid@alcor.concordia.ca.

General Questions

The following 8 questions are of a general nature. They are mainly meant for informational and demographical purposes.

1. **Which DRIE chapter do you belong to?**

○ **DRIE Atlantic**

○ **DRIE Montreal**

○ **DRIE Ottawa**

○ **DRIE Toronto**

○ **DRIE SW Ontario**

○ **DRIE Central**

○ **DRIE West**

2. **Which best describes your company's primary line of business?**

○ **Banking**

○ **Financial Services (e.g.: Real Estate, Insurance...) other than banking**

○ **Manufacturing (e.g.: Consumer/Industrial Goods)**

○ **Hotel**

○ **Tourism & Travel other than Hotel**

○ **Communications (e.g.: Media, Entertainment, Print...)**

○ **Construction (e.g.: Engineering...)**

○ **Public/Parapublic (e.g.: Education, Energy/Utility, Government, Healthcare...)**

● **Professional (e.g.: Legal, Consulting...)**

○ **Technology (e.g.: Services, Software/Hardware, Telecommunications...)**

○ **Services (e.g.: Transportation, Courier...)**

○ **Retail**

○ **Distribution**

○ **Other**

3. **What is your job title?**

4. **How many individuals are dedicated <u>full-time</u> to the BC/DR program?**

○ 0

○ 1 to 2

○ 3 to 5

○ Greater than 5

○ Do not know

5. **Which level champions the BC/DR program at your location?**

○ Executive level (e.g.: CEO, CIO, COO, CFO, Controller...)

○ Management level (e.g.: directors, managers, supervisors, team leaders...)

○ Operational level (e.g.: planners, coordinators, administrators...)

6. **Does your BC program differ from your DR program?**

○ Yes (they are 2 separate programs)

○ No (they are one and the same)

○ Mixed (programs are distinct but components of one may be components of the other

7. **How many people are employed...**

At your location?

○ 0 to 99

○ 100 to 499

○ 500 to 999

○ 1000 to 4999

○ greater than 5000

Throughout your organization?

○ 0 to 99

○ 100 to 499

○ 500 to 999

○ 1000 to 4999

○ greater than 5000

8. **At your location, what percent of total operational expenses is dedicated to the administration of your BC/DR program?**

○ Less than 1%

○ 1% to 2%

○ 2% to 5%

○ Greater than 5%

○ Unknown or unavailable

Business Continuity / Disaster Recovery Questions

The following 15 questions pertain to your BC/DR program within your location/organization.

9. **The BC/DR program was implemented with the cooperation of (please select all that apply):**

□ **Solely IT, or**

□ **Upper Management (e.g.: CEO, CIO, CFO, VPs...)**

□ **Middle and/or Lower management (e.g.: managers, directors, supervisors...)**

□ **Multi-disciplinarian teams (e.g.: individuals from IT, HR, Marketing, Finance...)**

□ **3rd party consultant/vendor (e.g.: Sunguard, CGI, etc.)**

□ **Other (please specify)**

10. **When did your firm decide to implement a BC/DR program?**

○ **Prior to January 1st, 2000**

○ **Between January 1st, 2000 and December 31st, 2002**

○ **Since January 1st, 2003**

○ **Do not know**

11. **Why did your corporation initially develop a BC/DR program?**

○ **Because of fears stemming from the January 1, 2000 computer rollover date ("Y2K")**

○ **Because of the events of September 11th, 2001 ("9/11")**

○ **Because of regulations (e.g.: Sarbanes-Oxley, HIPAA...)**

○ **Because of some other event**

Please describe

12. **Was an existing BC/DR program modified by the events from...**

	Yes	**No**
...Y2K	□	□
...9/11	□	□
...Regulations (e.g.: SOX, HIPAA....)	□	□
...Other (please specify)	□	□

□ **Not modified by any of the above**

13. Are your organization's internal policies given more importance than external policies (e.g.: laws, regulations, etc.)?

○ **Yes**

○ **No**

14. Since <u>January 1st, 2004,</u> has your location suffered a data loss due to any of the following (please select all that apply):

<u>Natural disasters</u>

□ ***Not suffered from any type of Natural disaster***

□ **Earthquake**

□ **Tornado**

□ **Ice storm**

□ **Hurricane**

□ **Flood**

□ **Lightning**

□ **Extreme Weather**

□ **Snow storm**

□ **Other**

<u>Human disasters</u>

Accidental **(not malicious in nature)**

□ ***Not suffered from any type of Human mishaps***

□ **Mechanical failure**

□ **Security mismanagement**

□ **Liquid spill**

□ **Inadequate contingency**

□ **Operating errors**

□ **Other**

Intentional **(malicious and meant to harm)**

□ ***Not suffered from any type of Human acts***

□ **Arson**

□ **Vandalism**

□ **Terrorism (or threat of)**

□ **Other**

□ **Riot**

□ **Sabotage**

□ **Bomb threat**

Technological disasters

Intentional **(malicious and meant to harm)**

□ ***Not suffered from any type of Technological Threats***

□ **Viruses & worms**

□ **Phishing**

□ **Spamming**

□ **Hacking**

□ **DoS attacks**

□ **Other**

Accidental **(not malicious in nature)**

□ ***Not suffered from any type of Technological Occurrences***

□ **Electrical/PC fire**

□ **Hardware failure**

□ **Software failure**

□ **Other**

□ **PC short-circuitry**

□ **O/S failure**

□ **Network failure**

□ **Power outage**

□ **Telecomm. failure**

□ **Service provider failure**

15. With respect to Question 10 above, what is your estimation of the total cost of this (these) event(s)? (in $CAN).

○ **Less than $100,000**

○ **Between $100,000 and $499,999**

○ **Between $500,000 and $999,999**

○ **Between $1 million and $5 million**

○ **More than $5 million**

○ **Do not know**

16. What procedure(s) are used to assess recovery? (please select all that apply).

□ Departmental tests

□ Corporate-wide test

□ Local business resumption/recovery

□ Alternate site business resumption/recovery

□ Crisis emergency/management

□ Mock disaster management

□ Specific application recovery

□ Test all critical systems

□ Redundant facilities and datacenters tested and used as primary for duration of test

□ Other □

17. Please rank the following recovery objectives for your location (1 being the most important):

	RANK
Recovering within budget	□
Recovering within time	□
Recovering according to business priorities	□

Please describe

□

18. Are the recovery objectives for your location the same as the recovery objectives for other locations in your firm?

○ Yes

○ No

○ Do not know

19. How do you measure the performance of your BC/DR program? (please select all that apply):

□ **Service level monitoring**

□ **Plan exercises (paper-based simulations, walkthroughs, etc.)**

□ **Audit findings**

□ **Performance reviews**

□ **Benchmarking**

□ **N/A - We do not measure performance**

20. How often do you test your DR/BC program?

○ **Annually**

○ **Semi-annually**

○ **Quarterly**

○ **Monthly**

○ **As needed**

○ **Never**

○ **Never but plan to test**

21. How often do you update your BC/DR program?

○ **Annually**

○ **Semi-annually**

○ **Quarterly**

○ **Monthly**

○ **As needed**

○ **Never**

○ **Never but plan to update**

22. In your opinion, do employees get sufficient BC/DR program related training at your location?

● **Yes**

○ **No**

23. Please indicate the level of importance to the BC/DR program of the following eighteen (18) factors. Please identify the top 5 which you deem most important in implementing an effective BC/DR program and rank these from 1 to 5 (1 being the most critical).

	LEVEL OF IMPORTANCE					RANKING
	Extremely	Very	Somewhat	Less	Not at all	(only top 5)
1. Top Management Commitment	○	○	○	○	○	□
2. Adequate Financial Support	○	○	○	○	○	□
3. Alignment of BCP/DRP Objectives with Company's Goals	○	○	○	○	○	□
4. Adoption of Project Management Techniques	○	○	○	○	○	□
5. Presence of Formal Recovery Planning Committee	○	○	○	○	○	□
6. Participation of Representatives from each Department	○	○	○	○	○	□
7. Engagement of External Consultant	○	○	○	○	○	□
8. Risk Assessment	○	○	○	○	○	□
9. Business Impact Analysis (BIA)	○	○	○	○	○	□
10. Determination of Maximum Allowable Downtime	○	○	○	○	○	□
11. Prioritization of IS Applications	○	○	○	○	○	□

12. Off-site Storage of Backup	○	○	○	○	○	□
13. Presence of Emergency Response Procedures	○	○	○	○	○	□
14. Training of Recovery Personnel	○	○	○	○	○	□
15. Appropriate Backup Site	○	○	○	○	○	□
16. Periodical Testing of BCP/DRP	○	○	○	○	○	□
17. Maintenance of BCP/DRP	○	○	○	○	○	□
18. Insurance Coverage for IS Loss	○	○	○	○	○	□

24. Recent research suggests additional factors to the 18 listed in Question #23. Regarding the additional factors, please indicate the level of importance for your firm and, if appropriate, whether the additional factor would rank in the top five considering all 21+ factors.

	LEVEL OF IMPORTANCE					RANKING
	Extremely	Very	Somewhat	Less	Not at all	(only top 5)
19. Service Level Agreements (SLAs)	○	○	○	○	○	□
20. Effective Communication	○	○	○	○	○	□
21. BC/DR Implementation Plan	○	○	○	○	○	□
22. Other (please specify)						
□	○	○	○	○	○	□
□	○	○	○	○	○	□
□	○	○	○	○	○	□

Thank you for taking the time to answer these questions

.

APPENDIX XXI E-mail Instructions to Complete Survey Questionnaire

[insert name of DRIE president],

Recently, we sent you an e-mail requesting your cooperation regarding a research questionnaire on the subject of Business Continuity/Disaster Recovery. We are grateful that you are willing to forward the questionnaire to your members. The questionnaire is now complete and we are including this document to you for distribution.

Attached you will find the following:

* The questionnaire (including a cover letter)
* A suggested message to send to your members (at then end of this message).

Please inform me of the number of members of your DRIE to whom this questionnaire has been sent. This information will be needed in order to calculate the various response rates from each DRIE. We do not need the list of e-mails, simply the number of members.

If you have any comments or questions concerning the questionnaire, the process, or this e-mail, please feel free to contact Michael at any time.

Many thanks and best regards,

Michael Barbara, CBCP
M.Sc.A., Concordia University
m_barbar@jmsb.concordia.ca

Dr. Kevin Laframboise
Assistant Professor, Concordia University
lafrak@jmsb.concordia.ca

[Suggested Letter by You, DRIE president]

Dear DRIE members,

One of our colleagues from DRIE Montreal, Mr. Michael Barbara, is completing his Master's of Science in Administration degree at Concordia University and is kindly requesting your assistance in completing his questionnaire on Business Continuity/Disaster Recovery (BC/DR).

Mr. Barbara is examining whether the critical success factors for implementing a BC/DR program have changed from previous research, specifically subsequent to the events of September 11th, 2001. As we all know, the events of 9/11 have altered the landscape of Business Continuity and its subset, Disaster Recovery, in multiple ways: increased regulations, rigourous testing and the proliferation of BC/DR jobs are only a sample of the consequences stemming from this event.

The questionnaire should take no more than 20 minutes to complete. It is important to stress that all results are strictly confidential and in no way will your name or any reference to your company be made.

There are 3 ways that you can complete this questionnaire and return it:

1. ON-LINE VERSION

You may complete the on-line version of the questionnaire by clicking on the link below:
http://www.surveymonkey.com/s.asp?u=95081138719

2. E-MAIL ATTACHMENT

You may download the Word document, save it to your hard drive (e.g.: on your Desktop), open and complete the questionnaire electronically, save your answers as "Completed Survey Document" and return it to the following e-mail address:
m_barbar@jmsb.concordia.ca
NOTE: The Word version may take some time to download due to its size.

3. REGULAR MAIL

You may open the .pdf file (you will need Adobe Acrobat to open this file) or Word document, print it, complete the survey and send it back to the following address :

John Molson School of Business - Concordia University
Michael Barbara research
c/o Dr. Kevin Laframboise
1550 de Maisonneuve O.
GM 209-39
Montreal, Quebec, Canada
H3G 1M8

It would be appreciated if the duly-completed questionnaire be submitted **no later than Friday December 16th, 2005**.

Mr. Barbara will be sending us the results, which may be beneficial to our DRIE.

If you have any comments, questions or concerns with respect to the latter, feel free to contact Michael at the following:

E-mail m_barbar@jmsb.concordia.ca

Regards,

Michael Barbara, CBCP
M.Sc.A., Concordia University
m_barbar@jmsb.concordia.ca
(450) 687-3255

Dr. Kevin Laframboise
Assistant Professor, Concordia Univeristy
lafrak@jmsb.concordia.ca

APPENDIX XXII Interview Variable Count of Critical Success Factors

INTERVIEW	CSF1	CSF2	CSF3	CSF4	CSF5	CSF6	CSF7	CSF8	CSF9	CSF10
Company A										
Interviewee 1	Q1*					Q3*				
Interviewee 2										
Interviewee 3						Q6*	Q3*	Q6*	Q3*	
Company B										
Interviewee 1	Q5*						Q4*		Q3* Q5*	
Interviewee 2					Q3*			Q2*	Q1* Q2*	
Interviewee 3	Q4*				Q5*		Q2* Q5*			
Company C										
Interviewee 1			Q1*			Q2*	Q4* Q6*			
Interviewee 2						Q5*	Q4*		Q1* Q2* Q3*	
Interviewee 3	Q1*					Q1*	Q1* Q3*			
Company D										
Interviewee 1 & 2	Q6**	Q6*	Q4* Q6*			Q4*	Q4*			
TOTAL COUNT	6	1	3	0	2	6	10	2	9	0
RANK							#4		#5	

INTERVIEW	CSF11	CSF12	CSF13	CSF14	CSF15	CSF16	CSF17	CSF18	CSF19	CSF20	CSF21
Company A											
Interviewee 1				Q3*			Q3*				
Interviewee 2	Q6*			Q3* Q6*		Q3*					Q3*
Interviewee 3				Q3* Q5*			Q5*				Q3*
Company B											
Interviewee 1				Q3*		Q3* Q6**	Q6*				Q6*
Interviewee 2						Q1* Q2* Q5* Q6**	Q6*				Q2*
Interviewee 3	Q2*			Q3* Q5*		Q3** Q4* Q6*	Q3** Q5* Q6*				
Company C											
Interviewee 1	Q1* Q3*				Q2*	Q1*** * Q2* Q4** Q6*** *	Q3* Q5***			Q1*	
Interviewee 2	Q1* Q2* Q3* Q4*			Q5* Q6*	Q1* Q2*** Q3*	Q1*** * Q3* Q4* Q5* Q6**	Q4* Q5*				Q5*
Interviewee 3						Q1** Q3* Q6**	Q1*			Q2*	
Company D											
Interv. 1 & 2			Q6*	Q6*		Q6*					Q6*
TOT. COUNT	**9**	**0**	**1**	**11**	**6**	**39**	**15**	**0**	**0**	**2**	**6**
RANK	**#6**			**#3**		**#1**	**#2**				

APPENDIX XXIII Ranking of Top Five CSFs from Current Study (Using Chow and Luk (1996) Methodology)

Rank	Order	CSF 1	CSF 2	CSF 3	CSF 4	CSF 5	CSF 6	CSF 7	CSF 8	CSF 9	CSF 10	CSF 11	CSF 12	CSF 13	CSF 14	CSF 15	CSF 16	CSF 17	CSF 18	TOTAL
1	a	**38**	3	1	0	0	2	0	0	2	0	0	1	1	0	3	1	0	0	52
	c	*																		
2	a	6	3	9	0	3	5	0	5	**8**	2	0	1	2	0	3	4	1	0	52
	b	--	6	10	0	3	7	0	5	**10**	2	0	2	3	0	6	5	1	0	
	c									*										
3	a	2	6	**3**	1	4	4	0	3	9	1	0	0	3	2	0	8	6	0	52
	b	--	12	**13**	1	7	11	0	8	--	3	0	2	6	2	6	13	7	0	
	c			*																
4	a	0	1	0	2	2	8	0	0	5	6	1	0	3	5	1	**11**	7	0	52
	b	--	13	--	3	9	19	0	8	--	9	1	2	9	7	7	**24**	14	0	
	c																*			
5	a	2	5	1	1	2	3	1	2	2	4	1	7	2	1	2	7	**9**	0	52
	b	--	18	--	4	11	22	1	10	--	13	2	9	11	8	9	--	**23**	0	
	c																	*		

RANKING

1	CSF 1	Top Management Support
2	CSF 9	Business Impact Analysis (BIA)
3	CSF 3	Alignment of BCP/DRP Objectives with Company Goals
4	CSF 16	Periodic Testing of BCP/DRP
5	CSF 17	Maintenance of BCP/DRP

APPENDIX XXIV Factor Analysis of Survey Data using SPSS

Component Matrix
1st iteration - 6 components extracted

Rotated Component Matrix[a]

Survey Question	**Component**						**Related Critical Success Factor**
	1	*2*	*3*	*4*	*5*	*6*	
Q28E	,916						Presence of Recovery Committee (CSF5)
Q28F	,916						Representatives from each Dept. (CSF6)
Q28N		,742					Training (CSF14)
Q28P		,658					Testing (CSF16)
Q28Q		,654					Maintenance (CSF17)
Q28R		,649					Insurance Coverage (CSF18)
Q28M		,592					Presence of ERPs (CSF13)
Q28J			,744				Maximum Allowable Downtime (CSF10)
Q28D			,642				PM Techniques (CSF4)
Q28I			,627				BIA (CSF9)
Q28K			,533				Prioritization of IS Apps. (CSF11)
Q28B				,777			Adequate $$ support (CSF2)
Q28C				,670			BC/DR obj. -> Company Goals (CSF3)
Q28A				,607			Top Mgmt Support (CSF1)
Q28G				,573			External Consultant (CSF7)
Q28L					,914		Offsite Storage of Backup (CSF12)
Q28O					,531	-,509	Appropriate Backup Site (CSF15)
Q28H						,727	Risk Assessment (CSF8)

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 15 iterations.

Realization: **Since Q28O has negative correlation between the 5th and 6th factors, it will be removed in the next iteration conversion.**

Component Matrix
2nd iteration - 6 components extracted

Rotated Component Matrix[a]

Survey Question	**Component**						**Related Critical Success Factor**
	1	*2*	*3*	*4*	*5*	*6*	
Q28E	,900						Presence of Recovery Committee (CSF5)
Q28F	,900						Representatives from each Dept. (CSF6)
Q28N		,738					Training (CSF14)
Q28P		,679					Testing (CSF16)
Q28Q		,672					Maintenance (CSF17)
Q28R		,641					Insurance Coverage (CSF18)
Q28M		,579					Presence of ERPs (CSF13)
Q28B			,786				Adequate $$ support (CSF2)
Q28D			,673				BC/DR obj. -> Company Goals (CSF3)
Q28A			,599				Top Mgmt Support (CSF1)
Q28G			,578				External Consultant (CSF7)
Q28J				,770			Maximum Allowable Downtime (CSF10)
Q28K				,668			Prioritization of IS Apps. (CSF11)
Q28D				,660			PM Techniques (CSF4)
Q28I				,551			BIA (CSF9)
Q28H					,843		Risk Assessment (CSF8)
Q28L						,912	Offsite Storage of Backup (CSF12)

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 9 iterations.

Realization: If we remove Q28L, we would remain with 5 sets of factors (components).

Component Matrix
3rd iteration - 5 components extracted

Rotated Component Matrix[a]

Survey Question	**Component**					**Related Critical Success Factor**
	1	*2*	*3*	*4*	*5*	
Q28N	,740					Training (CSF14)
Q28Q	,672					Maintenance (CSF17)
Q28P	,679					Testing (CSF16)
Q28R	,641					Insurance Coverage (CSF18)
Q28M	,579					Presence of ERPs (CSF13)
Q28E		,884				Presence of Recovery Committee (CSF5)
Q28F		,884				Representatives from each Dept. (CSF6)
Q28B			,758			Adequate $$ support (CSF2)
Q28G			,735			External Consultant (CSF7)
Q28C			,550			BC/DR obj. -> Company Goals (CSF3)
Q28A			,537			Top Mgmt Support (CSF1)
Q28J				,768		Maximum Allowable Downtime (CSF10)
Q28K				,749		Prioritization of IS Apps. (CSF11)
Q28I				,568		BIA (CSF9)
Q28D						PM Techniques (CSF4)
Q28L					,822	Offsite Storage of Backup (CSF12)

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 12 iterations.

Realization: **In order to reduce the number of components to 4, we remove the Q28L question.**

Component Matrix
4th iteration - 4 components extracted

Rotated Component Matrix[a]

Survey Question	**Component**				**Related Critical Success Factor**
	1	*2*	*3*	*4*	
Q28N	,752				Training (CSF14)
Q28Q	,725				Maintenance (CSF17)
Q28P	,712				Testing (CSF16)
Q28M	,626				Presence of ERPs (CSF13)
Q28R	,602				Insurance Coverage (CSF18)
Q28E		,877			Presence of Recovery Committee (CSF5)
Q28F		,877			Representatives from each Dept. (CSF6)
Q28J			,753		Maximum Allowable Downtime (CSF10)
Q28K			,707		Prioritization of IS Apps. (CSF11)
Q28I			,691		BIA (CSF9)
Q28D			,553		PM Techniques (CSF4)
Q28B				,733	Adequate $$ support (CSF2)
Q28G				,710	External Consultant (CSF7)
Q28C				,572	BC/DR objectives -> Company Goals (CSF3)
Q28A				,561	Top Mgmt Support (CSF1)

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 11 iterations.

Realization: **In order to ascertain that the number of components is 4 and to increase the respective alphas of each, we removed Q28R question (factor set #1), Q28D (factor set #3) and Q28G (factor set #4).**

Component Matrix
5th **iteration** - 4 components extracted
FINAL ITERATION

Rotated Component Matrix[a]

Survey Question	**Component**				**Related Critical Success Factor**
	1	*2*	*3*	*4*	
Q28P	,772				Testing (CSF16)
Q28N	,752				Training (CSF14)
Q28Q	,725				Maintenance (CSF17)
Q28M	,626				Presence of ERPs (CSF13)
Q28F		,877			Representatives from each Dept. (CSF6)
Q28E		,877			Presence of Recovery Committee (CSF5)
Q28J			,813		Maximum Allowable Downtime (CSF10)
Q28K			,779		Prioritization of IS Apps. (CSF11)
Q28I			,713		BIA (CSF9)
Q28B				,836	Adequate $$ support (CSF2)
Q28C				,659	BC/DR objectives -> Company Goals (CSF3)
Q28A				,627	Top Mgmt Support (CSF1)

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 11 iterations.

Realization: This matrix makes sense.

RELIABILITY ANALYSIS - SCALE (ALPHA)

CASE PROCESSING SUMMARY – ENTIRE DATA SET

		N	%
Cases	Valid	52	100.0
	Excluded(a)	0	.0
	Total	52	100.0

RELIABILITY STATISTICS – ENTIRE DATA SET

Cronbach's Alpha	N of Items
.832	18

FACTOR SUB-SET #1: "INTRINSIC" FACTORS

```
Item-total Statistics

                Scale          Scale        Corrected
                 Mean         Variance        Item-            Alpha
               if Item        if Item         Total           if Item
               Deleted        Deleted      Correlation        Deleted

Q14             8,1538         5,2700         ,6073            ,6478
Q16             8,4231         5,4646         ,5495            ,6689
Q17             8,5577         5,3888         ,6370            ,6441
Q18             7,2500         5,0931         ,3003            ,8031
Q13             8,3846         5,3002         ,5306            ,6722

Reliability Coefficients

N of Cases =      52,0                    N of Items =  5

Alpha =     ,7321
```

Realization: If Q18 deleted, then the Alpha would be ,8031 instead of ,7321

==

FACTOR SUB-SET #2: "INTRINSIC" FACTORS

```
Item-total Statistics

                Scale          Scale        Corrected
                 Mean         Variance        Item-             Alpha
               if Item        if Item         Total            if Item
               Deleted        Deleted      Correlation         Deleted

Q5              1,9231          ,4253         1,0000               .
Q6              1,9231          ,4253         1,0000               .


Reliability Coefficients

N of Cases =      52,0                      N of Items =   2

Alpha =    1,0000
```

===

FACTOR SUB-SET #3: "INTRINSIC" FACTORS

```
Item-total Statistics

                Scale          Scale        Corrected
                 Mean         Variance        Item-             Alpha
               if Item        if Item         Total            if Item
               Deleted        Deleted      Correlation         Deleted

Q10             6,6923         3,0799          ,6765             ,5241
Q4              5,8846         3,7119          ,3055             ,7610
Q9              6,7308         3,0241          ,5793             ,5809
Q11             6,5962         3,8533          ,4493             ,6673

Reliability Coefficients

N of Cases =      52,0                      N of Items =   4

Alpha =     ,7045
```

Realization: If Q4 deleted, then the Alpha would be ,7610 instead of current ,7045

===

FACTOR SUB-SET #4: “INTRINSIC” FACTORS

```
Item-total Statistics

               Scale          Scale        Corrected
               Mean          Variance        Item-              Alpha
              if Item        if Item         Total             if Item
              Deleted        Deleted      Correlation          Deleted

Q1             8,1346         4,0403          ,4389              ,5863
Q2             7,5000         3,6667          ,5939              ,4871
Q3             7,5385         4,2534          ,4421              ,5902
Q7             5,9038         3,3435          ,3465              ,6936

Reliability Coefficients

N of Cases =      52,0                    N of Items =  4

Alpha =     ,6546
```

Realization: If Q7 deleted, then the Alpha would be ,6936 instead of current ,6546

```
=======================================================================
```