Critical Dimensions of Disaster Recovery Planning

Leong Lai Hoong[1] & Govindan Marthandan[1]

[1] Graduate School of Management, Multimedia University, Cyberjaya, Selangor, Malaysia

Correspondence: Leong Lai Hoong, Graduate School of Management, Multimedia University, Cyberjaya, Selangor, Malaysia. E-mail: yvonnellh@gmail.com

Abstract

Disaster Recovery Planning (DRP) emerged in the 1970s, during the era of electronic data processing when mainframe systems were used to crunch data and provide reports for business analysis. The importance of DRP is undeniable especially after the 911 terrorism attack and many natural disasters experienced by many countries; much effort has then poured in to maintain a set of workable DRP. However, though high investment is allocated for information technology and DRP, there are still IT service outages interrupted the business, crippled the operations and impacted the overall organization long term strategic plan. Questions arose on why DRP could not ensure an uninterrupted IT service environment. This paper aims to study the critical dimensions impacting the development and maintenance of DRP process, specifically to understand the dimensions that contribute to a successful DRP that aims to minimize the impacts of IT service outages. This study used a theoretical model, technology-organization-environment framework (TOE) to explore the adoption of DRP process in financial institutions in Malaysia. Following IT service management concept, individual components that comprise of trading partner readiness, staff competency, roles and responsibilities were included in the study. This study evidenced that 8 dimensions were critical for the implementation of DRP, in which 2 of 3 individual components being studied were part of the lists. These 8 dimensions could be used as guidance for future successful DRP rollout and its ongoing maintenance activities; with the ultimate objective to minimize outage duration of IT services that support critical business.

Keywords: contingency planning, business continuity management, business continuity planning, business recovery planning, disaster recovery planning, IT service continuity management

1. Introduction

Organizations maintaining business dynamism and attain competitive edge in the global scene are getting challenging due to the demanding stakeholders and keen competition. Sustaining uninterrupted business operation is a key in an organization's strategic plan to maintain competitive edge. According to a study by University of Minnesota, 93% of firms that lose critical systems for more than 10 days file bankruptcy almost immediately; 80% of firms affected by a major incident are forced to close within 18 months (Finn, Guillot, & Taylor, 2006). After the 11th September 2001 attack on the World Trade Centre, rampant terrorist attacks and frequent uncontrollable natural disasters, most organizations now have greater awareness of various types of business interruptions (Gallangher, 2003) and they shift focus to the planning for continuity of businesses, ensuring businesses are resilient and deploying a fast recovery after an emergency (Virgona, 2010). Their ultimate objectives are to satisfy stakeholders' needs in addition to keeping in business for as long as they can. There are three broad categories of disasters that will impact a business (Finn et al., 2006): natural, technical and human inflicted disasters. Knowing the types of disasters and plan for it are critical tasks, however the real challenge in IT environment during a disruption is ensuring that employees can always stay productive and to recover the relevant critical IT services within tolerable timeframe. DRP has been in the life of IT folks for more than 40 years (since 1970s), but there is no meaningful tool to objectively and consistently measure the organization's readiness in recovery from a disaster and their state-of-preparedness (Scott Ream, 2002b). Therefore there is a need to understand the dimensions affecting the DRP implementation so that right level of investment and efforts is spent on the right factors in order to have a successful DRP process.

1.1 The Financial Industry in Malaysia

The financial industry is the life-line industry in Malaysia (Bank Negara Malaysia, 2010) and other nations as

they spur the growth and stability of economy. In this journey, business continuity management (BCM) and DRP are instrumental as they maintain economic activities by enabling the domestic and international financial transactions to go on and prevent widespread payment or settlement disorder during a disaster (Arduini & Morabito, 2010). IT has supported the massive changes in the ways financial business is conducted; creation of financial service and product innovation cannot be achieved without technology.

An IT operating environments, typically contains a wide range of diverse application services and infrastructure components that have often evolved and expanded over time. This results in a complex network of servers and islands of software applications that can be difficult and costly to manage. It impedes the agility of the IT environment and limits the efficiency and effectiveness of the IT operations (Mercury, 2004). It is the objective of ministry of finance to ensure a chain of stable financial systems in the country (Bank Negara Malaysia, 2012). BNM has issued two guidelines for IT continuity and business continuity management (Bank Negara Malaysia, 2004, 2008). However, many instances of IT interruptions still occurred along with the strict guidelines implemented: on 16th October 2006, Hong Leong Bank encountered an intermittent computer system outage for 5 days before a double national festivals in Malaysia (The Star, 2006). On 3rd July 2008, Bursa Malaysia, the stock exchange of Malaysia, suspended a full day stock trading following a trading system glitch; a similar computer system interruption also occurred in year 2006 (Raj, 2008). On 22nd December 2008, Bursa Malaysia suspended stock trading again in the afternoon for about 45 minutes due to technical issues, this was the second time in the week for a similar situation happened in the trading environment (Sarif, 2008). These incidents shook the investors' confident in the local bourses, financial market and brought inconveniences, and dissatisfaction to the bank customers and stakeholders.

1.2 Literature Review

DRP is a process focused on the development of a plan to recover IT components from disaster, it was characterized as reactive and focus only on recovery of hardware and facilities (Herbane, Elliott, & Swartz, 2004). DRP is the antecedent and it is a subset of business continuity management (BCM) that focuses on moving business operations over to a backup facility (Finn, et al.). Prior literatures recommended different number of phases to implement a BCM and DRP depending on the subject matter being focused in their respective studies (Leong & Marthandan, 2013). Literatures also showed that there were many guidelines and framework but there is no DRP implementation path; neither nor any specific tool and solutions to be rolled out into production to support the DRP (Davies, 2000; Wood, 2006). Interpretations of these reference materials differ depending on the readers' knowledge, expertise and experience. In addition, the intensity of information and references related to DRP overwhelm and confuse the implementers and blur their vision for DRP rollout.

Focus of prior DRP researches also include: assessing the possibility of moving BCM to the strategic level of the organizations to further preserve the business value (Herbane et al., 2004; Karim, 2011); identifying critical success factor for implementing BCM (Kelly, 2012); developing business impact analysis and risk assessment model for BCM implementation (Shrivastava, Payal, Kumar, & Tiwari, 2012); the kinds of interruptions from small service disruptions to full blown disasters and the types of recovery plans and activities. Chow listed 17 success factors to develop a DR plan from 4 industries: financial services, manufacturing, trading and hotel in Hong Kong (Chow, 2000). In which 5 top success factors were highlighted though the ranking may differs for different industries. They are top management support, adequate financial support, appropriate backup site, off-site storage of backup and training of recovery personnel.

According to Dogson, technology includes not only tangible artefacts but also the knowledge that enables it to be developed and used in many useful ways (Dodgson, 2000). DRP has been an important process in the IT environment, it is technology and IS innovations, following Dogson definition of technology. This study uses Technology-Organization-Environment (TOE) framework, one of Technology Diffusion Models to test the success level of adopting and implementing DRP process.

Literature analysis revealed that IT has been viewed and treated as a service (Kettinger & Lee, 1994). Businesses are raising their bar for level of IT services that resulting in the efficiency and effectiveness of IT management being put in the limelight of the top management. IT service management process implementations focus on four areas or 4Ps that stand for process, people, product and partner. This means that implementation of every IT process have to consider the development of process and configuration of toolset around the people and partner or vendor who execute the process steps. People and partner are grouped under 'Individual' dimension in this study and it should be tested for its relevance in an existing Technology Innovation Diffusion model, such as the TOE framework. This study also aims to test if TOE framework can be extended to include an individual dimension.

1.3 Purpose of This Study

This study aims to identify the critical dimensions influencing the implementation of DRP process for financial institutions in Malaysia, and to validate if the individual dimension can be added to the existing technology innovation diffusion model. This study will be contributing to the following areas: (1) As suggested by Kelly, there is lack of implementation model for BCM and DRP (Kelly, 2012) and a need to develop a DRP implementation approach by knowing the factors that influence its success or failure. (2) As suggested by Scott, there is no tool to measure the success of DRP (Scott Ream, 2002b), this study aims to develop an IT process acceptance model using an established academic model. (3) In line with the development of IT service management processes (OGC Official Site, 2008) and the context of IT as a service, there is a need to assess the relevance to include individual dimension in the TOE model. (4) It is the author's objective to study DRP in the financial industry in a developing country like Malaysia.

2. Theoretical Background

2.1 Disaster Recovery Planning (DRP)

During the electronic data processing era, the mainframe was introduced to the business world in the 1950s. The objective was to use computers in recording, classifying, manipulating and summarizing data. The operator of the computer environments realized the need to keep backup copies of critical data in order not to lose it. These activities were the predecessors of DRP. The DRP emerged at the late 1970s when the first standby systems and data centers were established with primarily concerned on mainframe systems (SunGuard, 2011). It is an IT function to mainframe batch applications (Hiatt, 2000). The literature on the topic of disaster recovery uses the terms "disaster recovery", "business continuity", and "contingency planning" interchangeably due to its similar benefits and objectives (Finn et al., 2006). The benefits of contingency planning are to minimize potential loss by identifying, prioritizing, and safeguarding those assets that need the most protection (Petroni, 1999). Over time, hardware and software have become more reliable, yet Internet vulnerability, viruses, and mal-ware have become the primary threats to the IT infrastructure. While DRP is still an important part of IT, the scope of recovery planning has grown to include most critical business functions (Finn et al., 2006).

For comprehensiveness, DRP was recommended to be scenario based (Dirtadian, 2008; Herbane, et al., 2004) and developed using a life-cycle approach (Petroni, 1999). Three DRP stages are recommended: systems analysis, system design and systems implementation (Petroni, 1999). In addition, many components have been included in a DR plan. Such as recovery facilities, key recovery personnel, supplies, documents and forms (Finn, et al., 2006).

2.1.1 Phases of DRP

DRP is a multi-phases process but the number of phases is different from one researcher to another (Leong & Marthandan, 2013). In a book on DRP for computer systems, the author recommended a 10-phase DR project (Toigo, 1996), 10 professional practices in BCM and DRP (DRII, 2008; Toigo, 1996); studies on 7-phase BCM approach (BCM Institute, 2009; Gallangher, 2003), 6-phase BCM approach (BCI, 2008), 4-phases BCM approach that includes planning for risk prevention and mitigation, emergency response, crisis restoration and program management (Ketterer, Price, & McFadden, 2007; Mainline Information System); and a case study recommended 3-phase DR contingency plans (Petroni, 1999). Despite the number of phases and activities proposed, the ultimate goals for DRP are to prepare the organization to prevent, respond and recover from any business interruptions by having some planned activities that were grouped into three to ten phases.

2.1.2 Critical Success Factors of DRP

Many prior studies discussed the components that made up DRP (Herbane, 2010) but few discussed the critical success factors of DRP. A researcher studied the critical factors of DRP in 4 industries in Hong Kong (i.e. banking, trading, manufacturing and hotels industry) and concluded 17 factors impacting DRP (Chow, 2000). In a conceptual paper, 27 critical success factors have been identified for BCM implementation; however, it needs further validation (Kelly, 2012).

2.1.3 DRP in Financial Industry

Highly regulated industries such as financial services and telecommunications are the most motivated industries to invest in DRP (Finn, et al., 2006). In Malaysia, the central bank mandated that board of director should have oversight to ensure enterprise resilience (Bank Negara Malaysia, 2004, 2008). Some countries require financial institutions to provide attestations of their risk management and business continuity preparations to their local supervisory body, such as Thailand, Singapore, Australia, Hong Kong and India (Australian Prudential Regulation Authority, 2007; Bank of Thailand, 2005; Herbane, 2010; Hong Kong Monetary Authority, 2002;

Monetary Authority of Singapore, 2003).

2.1.4 DRP Implementation

DRP is an IT function and governed under IT governance. In the IT world, project management methodology and system development life cycle were some of the governance framework to achieve IT objective. The main objective of the project-management method is to have a basic system to manage behaviours of people who work together to satisfy the needs of their customers (Johns, 1995). Projects should be initiated to develop the DRP for computers and communication resources (Toigo, 1996); this was concurred that a deliberately well-planned project management approach should be taken in order to have a successful project with regards to IT processes (Pink Elephant, 2006). IT project success rate will improve (Skulmoski, 2001) following competency and maturity of project management methodology in an organization. In order to ensure the relevance to the ever growing business and to ensure that it works as and when needed, the disaster recovery plan must be maintained and tested at a predefined frequency (Bank Negara Malaysia, 2004, 2008; Cegiela, 2006; Emmanuele, Damiano, Sandro, & Marco, 2007; Gibb & Buchanan, 2006; Menkus, 1988; OGC 's Authorized Authors, 2001; Toigo, 1996). It was also recommended that a frequent audit program is developed to ensure that the DRP is aligned with corporate and IT governance at all times.

2.2 IT Service Continuity Management (ITSCM)

The rise of IT service management (ITSM) focuses on providing quality IT services that align IT with the business goals (Cater-Steel, Tan, & Toleman, 2007). ITSM is process-oriented where companies often employ software tools in order to support or automate all or part of these processes (Kuamoo, 2006). IT service continuity management (ITSCM) is one of the ITSM processes, was an extension of DRP (OGC 's Authorized Authors, 2001). In addition to being a critical technical component of BCM, ITSCM has incorporated the critical phases from BCM into the traditional DRP functions (Loftness & Drapeau, 2007). ITSCM's goal is to support BCM and ensure the businesses could have the IT systems back as quickly as possible after a disruption. In the development of version 3 of ITSM processes, four components were core: process, people, product (or tool) and partner (or vendor). It's about developing process and procedure to manage the IT operation environment with the right product, people and vendor in place. This includes employee working on recovery of IT services and vendors who support them. As such, individual component has been introduced since then to reflect the importance of people (include partner) in the process development (OGC Official Site, 2008).

2.3 People Component

Innovation is a broad concept involving people, processes and technology by developing scales to measure new competence acquisition (Gaynor, 2002). It was referred as initiative, practices or something known by a person or other unit of adoption (Rogers, 1995). Role of people is instrumental in promoting innovation and people competency influenced the overall effectiveness of an organization. The competency was initially defined as knowledge, skills and attitudes (Yang, Wu, Shu, & Yang, 2006) but was further refined and linked to a couple of factors that are causally related to outstanding achievement and superiority in the job (McClelland, 1973; McClelland & Boyatzis, 1980). From the ITSM perspective, people factor are core in process development too. It is the objective of this research to study the criticality of people factor in process innovation adoption. They would be considered in an attempt to extend the TOE framework from technology, organization and environment to technology, organization, environment and individual framework.

2.4 Technology-Environmental-Organization Framework

Technology has been referred to as a means of systematic knowledge transformed into tools and is considered instrumental in determining the efficiency which elements in a society are able to accomplish their tasks (Tornatzky & Fleischer, 1990). Definition of technology varied from physical components like hardware to open definitions that include software, human skill and organizational aspects of technology (Drejer, 2000). Technology is derived from human knowledge to be used for business operations to improve reliability, flexibility, productivity, efficiency and effectiveness in order to achieve business goals. Different organizations may decide to use different types of technology depending on the type of business, requirements of business for technology and organizations' strategic direction (Phoommhiphat, 2011). Innovation is anything that is new to an organization (Drucker, 1998) and it was adopted into an organization to improve its business and operational performance (Oke, Burke, & Myers, 2007; Zhongming, 2005) and enhanced abilities to offer products or services to customers (Peter, 2003). From the above definitions of technology and innovation, DRP is an innovation, a process innovation. DRP creates or improves the administrative operations and support the organization's core business. Therefore, this research would base on Swanson's IS innovation model and Tornatzky & Fleischer's "Technology-Organization-Environment framework" to explain the characteristics in

which a firm embraces and implements DRP process, a technological innovation.

2.4.1 Technology Context

DRP focuses on the availability of services during the service hour agreed with customers; should there be outages, proper and well tested processes and procedures are in place to recover such services within the agreed timeframe (Lawler & Szygenda, 2007; OGC 's Authorized Authors, 2001; OGC Official Site, 2008). Technology readiness refers to not only the underlying physical assets but also the availability of resources to support the services (T. Teo, Tan, & Wong, 1998). They should also be reliable (Lippert & Govindarajulu, 2006) to carry out its function as needed.

Disaster related behaviour is very complex, due to its occurrence at different social times in the life of different communities (Quarantelli, 1999). Many assume that there are insurmountable tasks to complete DRP process implementation, in addition to handling the on-going daily business at primary business premises. In order to achieve a smooth and efficient recovery, technology recovery involves the systematic and sequential recovery of hardware, software, data, network and backup technologies (Dirtadian, 2008; Jon Toigo, 1996; Serrelis & Alexandris, 2007; Toigo, 1996). Implementing DRP process is a complex and expensive undertaking (Gallangher, 2003).

The technology recovery involves a series of recovery efforts for physical assets, hardware, software, data, network and backup technologies that underpin the IT services (Serrelis & Alexandris, 2007; Toigo, 1996). The backup technologies are not only confined to equipment, they should also consider the building where the technology assets are sitting in and the facility that supports the IT services (Dirtadian, 2008; Ling, 1997). In order to strengthen organization competitive edge, technology integration and readiness (Oliveira & Martins, 2010) help improve firm accomplishment and performance by having shorter recovery time, more satisfied customer service functions and lowered operations costs.

2.4.2 Organizational Context

An acceptable level of service quality was one of the most important objectives for implementing DRP process (Gronroos, 1984). It is the expectation of all customers to experience uninterrupted services provided by the organizations; and that the products, services or internal processes are being continuously improved to satisfy the ever changing customer needs (Chau & Tam, 1997; Iacovou, Benbasat, & Dexter, 1995; Lippert & Govindarajulu, 2006; Oliveira & Martins, 2010; Ramdani, Kawalek, & Lorenzo, 2009; T. S. H. Teo, Lin, & Lai, 2009).

Organizational compatibility refers to the implementation of DRP is in harmony with the organization's practice, value and culture. The presence of organization policy and framework will certainly support the implementation of DRP. Such as, learning and development policy, internal and external communications policy, management risk position, technical blueprint and technology process frameworks like System Development Life Cycle (SDLC) (Chau & Tam, 1997) or Project Management Methodology (Iacovou et al., 1995; Ifnedo, 2011; Ramdani et al., 2009; T. Teo et al., 1998; T. S. H. Teo et al., 2009; Zhu, Kraemer, & Xu, 2005).

Top management support and decision-maker characteristics were one of the important dimensions within the organizational context to support diffusion of technology in an organization (Ifnedo, 2011; Ramdani et al., 2009; T. Teo et al., 1998; T. S. H. Teo et al., 2009; Thong, 1999; Wang, Wang, & Yang, 2010). Mitroff stressed that no human being, business, organization or institution can continue to survive for long period without presence of quality leadership during the crisis (I. Mitroff, 2005). It was also recommended that senior management should be responsible for DRP implementation which includes robust plan development, a well-tested and well-communicated plan to all stakeholders (Woodman, 2008).

2.4.3 Environment Context

External pressures to the survival of the organization and business growth are one of the critical environmental factors influencing the decision to adopt IS innovation (Iacovou, et al., 1995). External pressures could further breakdown into information intensity, competitor pressure, industry competition, regulatory requirement and government support (Kuan & Chau, 2001; T. Teo, et al., 1998; Zhu, Xu, & Dedrick, 2003).

IT services are underpinned by physical and technology infrastructure. They include building location, security of the location, protection equipment such as fire prevention devices, fire and theft alarm, location monitoring systems; and data center utilities such as cooling system, hardware rack and cabling management (Khalil & Elmaghraby, 2008; Wadekar, 2007; Wiboonrat, 2008).

Consumers are cognizant of the types of IT services they buy and their rights as IT users. Service Level

Agreement (SLA) describes the specifications of IT services traded and set the expectations of customers of the kind of service level they will receive for the price they pay (OGC 's Authorized Authors, 2001; OGC Official Site, 2008). SLA also ensures that customer rights are protected and that they receive the high quality of IT services (Voas & Wilbanks, 2008). Business environmental characteristics include the supply chain of doing business. They are the organization's suppliers, business partners, customers and the industry practitioners. In the practitioner world, Scott recommended the maturity level of BCM as a control for DR policy and plan adherence (Scott Ream, 2002a, 2002b).

2.4.4 Individual Context

Successful business characteristics include the readiness of supply chain in doing business, such as the organization's supplier, business partners, customers and the industry practitioners. For enterprise resiliency, it was suggested to focus on the resilience of critical assets which include human resources, staff and third party relationships instead of developing only a scenario-based plan (Dirtadian, 2008; Herbane, et al., 2004).

DRP is an IT process to prepare IT folks on how to respond to system outages that may impact IT users and organizations. It defines the procedure, roles and responsibilities required to respond immediately should a system outage occur (Bank Negara Malaysia, 2004, 2008). BCM and DRP set out clear roles and responsibilities (Emergency Planning Unit, 2006). All managers and employees should be aware of their duties in the event of a disruption and therefore the roles and responsibilities need to be documented clearly, communicated and employees are trained in recovery tasks (Woodman, 2008).

IT human resources provide the skills and knowledge to recover IT services (Zhu et al., 2005). Many authors emphasized the stages of a crisis: either pre-or post-crisis planning with the right level of staff and the strategic plan that is needed to respond to the crisis (Hickman & Crandall, 1997; I. I. Mitroff & Pauchant, 1990). The disaster recovery plan should also address the people and skills needed for recovery tasks, which it remains a gap in many organizations (Woodman, 2008).

3. Research Methodology

The goal of this research is to identify critical dimensions impacting DRP process and to investigate their relationships. From literature discussed above, the research framework was described in figure 1 below (Leong & Marthandan, 2011). To achieve the goals of this study, twelve hypotheses are developed as in figure 2 below.
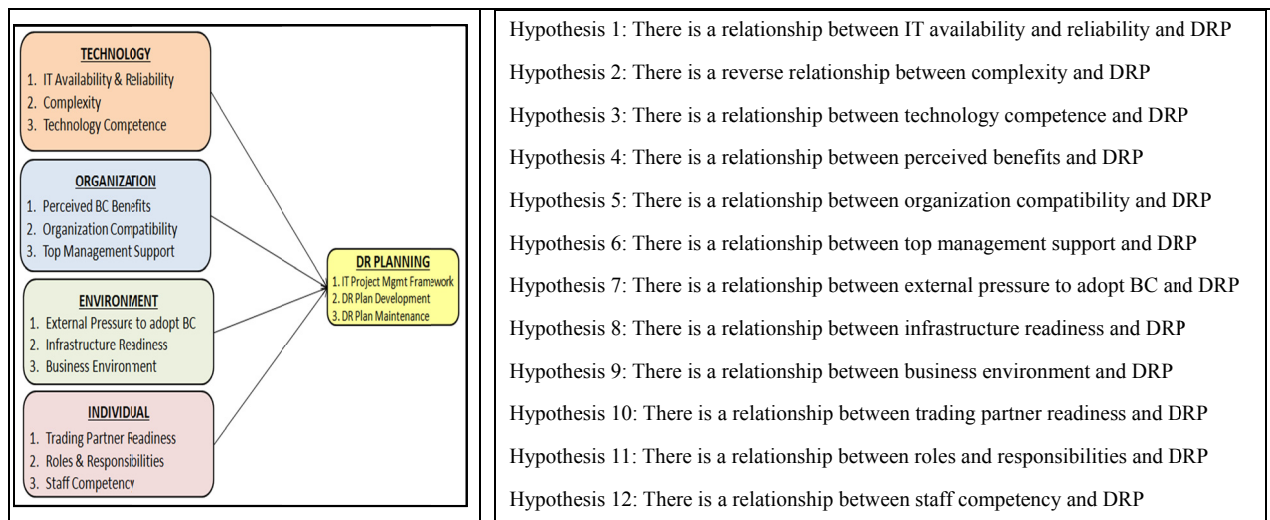

Figure 2. Hypothesis for this study

3.1 Sampling Strategy

In this research, the population is made up of the BCM and DRP subject matter experts from the financial institutions in Malaysia. They are personnel involving in developing and maintaining the BCM and DRP of the organization. This research aims to confirm the theoretical framework which exploratory and confirmatory analyses of the structural equation modelling (SEM) method are required. To use SEM tools, the recommended sample size ranges from 100 units (Haenlein & Kaplan, 2004), to 200 units in order to have a sufficient level of

degree of confidence in estimating parameter (Gerbing & Anderson, 1993). The unit of analysis is the individual staff working in the financial institutions. The sampling method used in this research is purposive sampling: a nonprobability sampling that enables the researchers to use their discernment to pick samples who have the best knowledge to progress the research, which is to fulfill the objectives of the research by answering the research questions.

3.2 Data Collection

This research employed email method to administer questionnaires after considering some recommended criteria (Saunders, Lewis, & Thornhill, 2009) such as: efficiency in reaching respondents in different geographical area; prospective respondents are computer-literate and have a business email id; higher confidence that the right person is identified and possibly would reply; suitable for close-ended questions which this research employs and available time available for data collection.

In this research, 84 organizations were successfully engaged where the names of the persons in charge of IT, BCM, Audit, Risk management and Operations were obtained. 1 to 5 respondents were identified from each organization. As a result, 316 questionnaires were sent via email to invite the targeted samples to participate in the survey. With an email reminder sent a week later and a phone calls made two weeks after the first email invite, 218 respondents replied. This came to a response rate of 69%. After screening the replies for survey completeness, only 208 responses were useable. As this is above 200 units, the critical sample size for analysis using SEM (Garver & Mentzer, 1999; Hoelter, 1983; Kline, 2005), it was adequate for this research.

4. Results

Data analysis was done in two stages. The first stage, preliminary data analysis has the objective of fine tuning the instrument in order to obtain a technically sound instrument for this research. The second stage is the final test which descriptive statistic and analysis were performed, such as frequencies, percentages and means to summarize demographic information. This was followed by factor analysis as a precursor to structural equation modeling (SEM) to confirm the grouping of items plus factors, and prepare for measurement model evaluation. A structural model developed is used to confirm the conceptual model and testing of research hypothesis.

4.1 Preliminary Data Analysis

The preliminary data analysis phases of the research process are needed to help the development of survey questionnaire (Babbie, 2001; Hussey & Hussey, 1997; Sekaran, 2003). Three instrument validation phases were performed in this research. (1) Content validation phase – practitioners and academicians familiar in the subject matters of BCM and DRP were invited to evaluate the questionnaires, appraise the form and validate the content. (2) Pre-test the questionnaire - an exercise to evaluate the comprehensibility of questionnaire. 10 professionals in the BCM and DRP areas were invited to perform a trial run of the questionnaire. Their feedbacks related to their overall feel, experience as a survey candidate and understanding of the questions were captured and used for instrument improvement. This is necessary to know if the questionnaire will be successful (Saunders et al., 2009). (3) Fifty candidates were invited to perform a pilot test to validate the reliability and construct of the instrument. After these three validation phases, the questionnaire was considered good to proceed to the final data gathering stage.

4.2 Final Test

Data collected during final data gathering stage were screened for removal of blank responses and outliers. Two basic assumptions in multivariate analysis (Tabachnick & Fidell, 2001) were achieved: data normality test and multicollenearity tests were performed to ensure data assumed normal and free from multicollienarity problem. Goodness of data was tested using inter-item correlation and Cronbach's Alpha reliability tests. Items were dropped to ensure that the inter-item correlation matrixes were greater than 0.3 and less than 0.9 to indicate the distance of the two items are sufficient to represent the variable but not too closely related (Hair, Black, Babin, & Anderson, 2010). The item's Cronbach's Alphas ranges above 0.6 are acceptable especially in the exploratory research (Hair et al., 2010). A factor analysis was then performed on the reduced number of items with principal components extracted. The factor loading of each of the item was greater than 0.7 to demonstrate an acceptable level of correlation and convergence between two items. KMO (Kaiser-Meyer-Olkin measure of sampling adequacy) was greater than 0.6 demonstrated internal consistency and adequate convergence between two concepts (Hair et al., 2010). The result was presented in Table 1 below.

Table 1- Initial Data Analysis Result

Constructs	Code	Cronbach's Alpha	KMO
IT availability & reliability	T1	0.910	0.845
Complexity	T2	0.874	0.600
Technology competence	T3	0.950	0.916
Perceived BC benefits	O1	0.845	0.600
Organizational Compatibility	O2	0.914	0.758
Top Management Support	O3	0.909	0.757
External pressure to adopt BC	E1	0.910	0.758
Infrastructure readiness	E2	0.822	0.700
Business environment	E3	0.870	0.600
Trading partners readiness	I1	0.920	0.858
Roles & responsibilities	I2	0.887	0.748
Staff competency	I3	0.778	0.600
DR Planning	DR	0.935	0.941

Table 2 - Structural Equation Modelling Result

	CMIN	DF	CMIN/DF	CFI	TLI	RMSEA
Thresholds	-	-	<3	>0.90	>0.90	<0.08
Technology	66.351	41	1.618	0.986	0.981	0.055
Organization	23.136	17	1.361	0.994	0.990	0.042
Environment	10.047	17	0.591	1.000	1.013	0.000
Individual	44.476	24	1.853	0.982	0.972	0.064
DR Planning	14.765	14	1.055	0.999	0.999	0.016
Measurement Model	876.15	782	1.120	0.986	0.983	0.024
Structural Model	1461.132	848	1.723	0.907	0.901	0.059

Subsequently, the data was put under structural equation modeling testing in which measurement model and structural model analyses were performed. During the measurement model analysis, each construct in the conceptual model (or measurement model) will be validated in Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) for evidence of construct validity and satisfactory levels of measurement model goodness-of-fit. The respective construct as a whole was examined using EFA and principal component approach, with threshold value of 0.3 and using varimax rotation. Convergent validity was examined by analyzing the factor loadings of the individual item loadings. A large standardized loading (>0.7) confirms that the indicators are greatly related to the constructs associated to it, thus convergent. For discriminant validity the variables should be significantly loads onto one factor; and if variable loads on multiple factors, the loading on each of the factor should differ by more than 0.2. In each of the construct measurement model, it was evidenced that Technology, Organizational, Environmental and Individual constructs each consists of 3 variables and respectively all their items loaded into one factor with high factor loading above 0.8 therefore satisfy convergent and discriminant validity. During CFA test, goodness-of-fit index used were Normed chi-square ($\chi^2/df<3$), Comparative fit index (CFI>0.9), Tucker-Lewis index (TLI>0.9) and Root Mean Square Error of Approximation (RMSEA<0.08) (Hair et al., 2010). Average variance extract (AVE), an indicator for convergence to be greater than 0.5 for convergence adequacy (Hair et al., 2010) and composite reliability (CR), a more precise reliability index in SEM models to be greater than 0.7 for high construct reliability or evidence of existence of internal consistency, but greater than 0.6 is acceptable (Hair et al., 2010). The data satisfied all CFA tests with model goodness-of-fit result presented in table 2 above.

Following the acceptance of the structural model, the hypotheses were tested. Table 3 below is the hypothesis testing table that was extracted from the standardized and unstandardized regression weight table of the AMOS reports. P-value less than 0.05 indicates significant hypothesis and as evidence for acceptance of hypothesis.

Table 3- Hypothesis Testing table

Independent Variables		B	Beta	P	Hypothesis
T1	IT Availability & Reliability	0.132	0.187	0.008	Supported
T2	Complexity	0.028	0.101	0.503	Not Supported
T3	Technology Competence	0.118	0.191	0.009	Supported
O1	Perceived BC Benefits	0.141	0.209	0.019	Supported
O2	Organization Compatibility	0.034	0.043	0.512	Not Supported
O3	Top Management Support	0.197	0.277	***	Supported
E1	External Pressure to Adopt DRP	0.153	0.282	***	Supported
E2	Infrastructure Readiness	-0.030	-0.042	0.567	Not Supported
E3	Business Environment	0.188	0.226	0.001	Supported
I1	Trading Partner Readiness	0.069	0.113	0.093	Not Supported
I2	Staff Competency	0.178	0.274	***	Supported
I3	Roles & Responsibilities	0.293	0.211	***	Supported

Table 4 – Ranking of Independent Variables

Independent Variables		Beta	Rank
E1	External Pressure to Adopt DRP	0.282	1
O3	Top Management Support	0.277	2
I2	Staff Competency	0.274	3
E3	Business Environment	0.226	4
I3	Roles & Responsibilities	0.211	5
O1	Perceived BC Benefits	0.209	6
T3	Technology Competence	0.191	7
T1	IT Availability & Reliability	0.187	8

5. Discussion

The results above fulfill the first objective of the research to identify the critical dimensions influencing the implementation of DRP process for financial institutions in Malaysia. Reference to table 3 above, the critical

dimensions influencing the implementation of DRP are IT availability and reliability, technology competence, perceived business continuity benefits, top management support, external pressure to adopt DRP, business environment, staff competency, roles and responsibilities as they have relationships with DRP as evidenced from the hypotheses. Table 4 above shows the ranking of impacts for all these factors to DRP. External pressure, top management support and staff competencies are the top three critical dimensions impacting DRP. These were followed by business environment, roles and responsibilities, perceived BC benefits, technology competence and IT availability and reliability. On the other hand, complexity, organization compatibility, infrastructure readiness and trading partner readiness are not critical dimension for implementing DRP as their hypotheses were not supported by the data. The result above also shows that the 2 of 3 variables from the individual dimension (staff competency and roles and responsibilities) were among the critical dimensions influencing the DRP process implementation. This answer the second objective of this research which is individual dimension is important and it can be added to the existing TOE framework.

The above identified critical dimensions impacting DRP process implementation were as expected and align with most if not all prior researches. However, the non-identified critical dimensions of DRP may have mixed findings as compared with prior researches. For complexity factor, some prior researches support the claim of complexity of innovation encourages the adoption of the innovation (Wang et al., 2010) but some reject the claim (Chau & Tam, 1997). Which the decision factor depends on the type of IS innovation being studied. For this research, the complexity of DRP process could sometimes be underestimated and level of complexity was unintentionally reduced to match the organization's capability level. Since DRP is mandatory for financial institutions in Malaysia, the management don't see any complexity issue while implementing DRP and they resolve to have it in place at all cost. For organization compatibility factor, there were mix findings from prior research: (Wang et al., 2010) support the claim but (Lin & Lin, 2008) reject the claim. In an organization, there are many types of frameworks and governance that can work independently with little or no overlapping. It is not a pre-requirement to have any types of framework and governances in place before DRP implementation. But it is one of its deliverables to produce a disaster recovery framework at the early stage in order to guide the development and implementation of DRP. Infrastructure readiness also refers to the readiness of local utility service providers. It is a good practice to build critical business space like data centre at a location equipped with backup resources like having dual in-coming source of utility (Finn et al.). However, this is not mandatory as there are many strategies to ensure the incoming utility supply are stable and not interrupted; such as installing power generator and telecommunication lines run by different service providers. There are always alternatives to ensure minimum disruption due to infrastructure. Such as performing a site risk assessments to understand the neighborhood where the business location is in and to remediate any unacceptable risks, if any. Therefore, infrastructure readiness needs not to be a critical dimension of DRP. Trading partner readiness refers to the knowledge, expertise and experiences the trading partner posses. Such as their abilities to participate in the DRP related activities discussion, sharing of DRP process, DRP simulation, business impact analysis and continuity improvement plan. The result of this study indicates an insignificant influence between trading partner readiness and DRP success. This result is in line with most literature if not all (Lin & Lin, 2008; Wang et al., 2010) .

In summary, this study addressed some suggestions from prior researchers and contributed to the DRP industry. It presents a model for DRP implementation with 8 critical dimensions that addressed Kelly's suggestion for a need to have a disaster recovery and business continuity management implementation approach by knowing the factors that influence its success or failure (Kelly, 2012). Knowing the critical factors impacting a project to implement DRP process, managers can put more efforts and focus in them to ensure a successfully project delivery, and proper DRP maintenance after going live. This is an IT process acceptance model developed using an established academic model, TOE framework; and that it can serve as a tool to guide a successful implementation of DRP in an organization (Scott Ream, 2002b). Arising from the development of ITIL processes (OGC Official Site, 2008), individual factor has also been considered for inclusion in an academic model (TOE framework in this study); it is evidenced in this study that staff competency, roles and responsibilities indeed are critical in process implementation and could be included in future studies using TOE framework. More importantly, this DRP implementation model was performed on the financial industry in a developing country like Malaysia, which has not been attempted in prior researches.

6. Limitations and Future Work

Similar to other studies, this study has some areas that could not be addressed. This study focused on only one specific industry, the financial industry of a developing nation, Malaysia. While focusing on one industry allows for control of extraneous industry factors that could confound the analysis, the results could not be represented and applied to other industries and regions. Also, the implementation approach may differ between organizations

in the East and in the West or between organizations in the developed and developing countries. However it is believed that the framework could be extended to other industry settings as the IT model demonstrated, the factors considered in the research were generic for all IT environment and technology setup. Respondents' attitudes play a vital role in the quality of this study. In view of most people who are busy with personal priorities, it raised concerns that the respondents did not spend the right level of time to consider the research questions and possible answers that best suit their organization.

There are few recommendations for considerations in future researches. This study was conducted on a financial landscape of a developing country; in order to generalize findings to a wider scope, further study can be conducted based on similar research issues on other industry, or in other countries. This study focus on the critical dimensions of DRP, it may lead to questions on the value of DRP to the organization. Therefore, this research model can be extended to explore the value DRP brings to the organization and its importance on the IT and business strategy map, basing on the critical dimensions discussed. In order to cover a more holistic view, it is recommended to also consider the view of customers, vendors and competitors in future research. Individual dimension was first introduced to TOE framework in this study. More researches of different IS innovation types and different industry could be considered to confirm the extended TOE framework.

References

Arduini, F., & Morabito, V. (2010). Business Continuity and The Banking Industry. *Communications of the ACM, 53*(3). http://dx.doi.org/10.1145/1666420.1666452

Babbie, E. (2001). *The Practice of Social Research*. Belmont, C.A.: Wadsworth.

Bank Negara Malaysia. (2004). *GPIS1-Guidelines on Management of IT Environment*. Retrieved from http://www.bnm.gov.my

Bank Negara Malaysia. (2008). *Guidelines on Business Continuity Management*. Retrieved from http://www.bnm.gov.my

Bank Negara Malaysia. (2010). About the Bank. from http://www.bnm.gov.my/index.php?ch=7&pg=735&ac=641

Bank Negara Malaysia. (2012). Financial Stability and Payment Systems Reports.

Bank of Thailand. (2005). Guideline for the Preparation of Information Technology Contingency Plan (IT Contingency Plan).

BCI. (2008). BCM Good Practices Guidelines. Retrieved 21 Aug, 2008, from http://www.thebci.org/

BCM Institute. (2009). BCM Body of Knowledge (BCMBoK). from http://www.bcm-institute.org/bcmi10/en/our-credentialing-process/bcm-body-of-knowledge

Business Continuity Management Guidelines. (2003).

Cater-Steel, A., Tan, W. G., & Toleman, M. (2007). *It SMF Australia 2007 Conference: Summary of ITSM Standards and Frameworks Survey Responses (ITIL Adoption Survey-2007)*. USQ & itSMF Australia.

Cegiela, R. (2006). *Selecting Technology for Disaster Recovery*. Paper presented at the Dependability of Computer Systems, 2006. DepCos-RELCOMEX '06. International Conference on.

Chau, P. Y. K., & Tam, K. Y. (1997). Factors affecting the adoption of open systems: an exploratory study. *MIS Quarterly, 21*(1). http://dx.doi.org/10.2307/249740

Chow, W. S. (2000). Success factors for IS disaster recovery planning in Hong Kong. *Information Management & Computer Security, 8*(2), 80–87. http://dx.doi.org/10.1108/09685220010321326

Davies, M. (2000). ITSM White Paper.

Dirtadian, L. (2008). Resilience and Change: Ten Tips for Making the Transition. *CPM Global Assurance*.

Dodgson, M. (2000). *The management of technological innovation: an international and strategic approac*. Oxford University Press.

Drejer, A. (2000). Integrating Product and Technology Development. *European Journal of Innovation Management, 3*(3). http://dx.doi.org/10.1108/14601060010334885

DRII. (2008). Professional Practices for BC Professioners. Retrieved from https://www.drii.org/professionalprac/index.php

Drucker, P. F. (1998). Management's New Paradigms. *Forbes, 162*(7).

Emergency Planning Unit, E. S. D. (2006). BC Guide for Small Business-Wiltshire County Council. Retrieved from http://www.wiltshire.gov.uk/business-continuity-guide-for-small-businesses.pdf

Emmanuele, Z., Damiano, B., Sandro, E., & Marco, S. (2007). *A Model Supporting Business Continuity Auditing and Planning in Information Systems*. Paper presented at the Proceedings of the Second International Conference on Internet Monitoring and Protection.

Finn, A., Guillot, J., & Taylor, J. (2006). Essentials of Disaster Recovery Planning.

Gallangher, M. (2003). Business Continuity Management - How to protect your company from danger. Retrieved from http://pqm-online.com/assets/files/lib/gallagher.pdf

Garver, M. S., & Mentzer, J. T. (1999). Logistics research methods: Employing structural equation modeling to test for construct validity. *Journal of Business Logistics, 20*(1).

Gaynor, G. H. (2002). *Innovation by Design: What it Takes to Keep Your Company on the Cutting Edge*. New York, NY.: AMACOM American Management Association.

Gerbing, D. W., & Anderson, J. C. (1993). *Monte Carlo evaluations of goodness-of-fit indices for structural equation models*. Sage Focus Editions.

Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management, 26*(2), 128–141. http://dx.doi.org/10.1016/j.ijinfomgt.2005.11.008

Gronroos. (1984). A Service Quality model and its market implications. *European Journal of Marketing, 18*(4), 36–44.

Haenlein, M., & Kaplan, M. A. (2004). A Beginner's Guide to Partial Least Squares Analysis.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis* (7th ed.). Pearson.

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History, 52*(6), 26. http://dx.doi.org/10.1080/00076791.2010.511185

Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business Continuity Management: time for a strategic role? *Long Range Planning, 37*(5), 435–457. http://dx.doi.org/10.1016/j.lrp.2004.07.010

Hiatt, C. J. (2000). A primer for disaster recovery planning in an IT environment: Idea Group Inc (IGI).

Hickman, J. R., & Crandall, W. R. (1997). Before disaster hits: A multifaceted approach to crisis management. *Business Horizons, 40*(2), 75–79. http://dx.doi.org/10.1016/S0007-6813(97)90013-6

Hoelter, D. R. (1983). The analysis of covariance structures: Goodness-of-fit indices. *Sociological Methods and Research, 11*.

Hussey, J., & Hussey, R. (1997). *Business Research: A Practical Guide For Undergraduate and Postgraduate Student*. Great Britain: Macmillan Press Ltd.

Iacovou, C. L., Benbasat, I., & Dexter, A. S. (1995). Electronic data interchange and small organizations: adoption and impact of technology. *MIS Quarterly, 19*(4), 465–485. http://dx.doi.org/10.2307/249629

Ifnedo, P. (2011). An Empirical Analysis of Factors Influencing Internet/ e-business Technologies Adoption by SMEs in Canada. *International Journal of Information Technology & Decision Making, 10*(4).

Johns, T. G. (1995). Managing the behavior of people working in teams. Applying the project-management method. *International Journal of Project Management, 13*(1), 33–38. http://dx.doi.org/10.1016/0263-7863(95)95701-E

Jon Toigo, W. (1996). *Disaster Recovery Planning For Computers and Communication Resources*. John Wiley & Sons, Inc.

Karim, A. J. (2011). Business Disaster Preparedness: An Empirical Study for measuring the Factors of Business Continuity to face Business Disaster. *International Journal of Business & Social Science, 2*(18), 183–192.

Kelly, M. (2012). Isolating CSF for Effective BCM-A Theoretical Review. *Journal of Business Continuity & Emergency Planning, 6*(1).

Ketterer, J. J., Price, B. J., & McFadden, A. C. (2007). The Business Continuity Plan: Outline for School Disaster Recovery. *International Management Review, 3*(4), 5–11.

Kettinger, W. J., & Lee, C. C. (1994). Perceived Service Quality and User Satisfaction with the Information Services Function. *Decision Sciences, 25*(5–6), 737–766.

http://dx.doi.org/10.1111/j.1540-5915.1994.tb01868.x

Khalil, Y., & Elmaghraby, A. S. (2008). *Data Center Resilience Evaluation Test-bed: Design and Implementation.* Paper presented at the Signal Processing and Information Technology, 2008. ISSPIT 2008. IEEE International Symposium on.

Kline. (2005). *Principles and practices of Structural Equation Modelling*. New York: The Guilford Press.

Kuamoo, P. K. J. (2006). *A framework for evaluating IT service management software products.* Unpublished M.Eng., University of Louisville, United States—Kentucky.

Kuan, K. K. Y., & Chau, P. Y. K. (2001). A perception-based model for EDI adoption in small business using a technology-organization-envionment framework. *Information and Management, 38*(8), 507–512. http://dx.doi.org/10.1016/S0378-7206(01)00073-8

Lawler, C. M., & Szygenda, S. A. (2007). *Components of Continuous IT Availability & Disaster Tolerant Computing.* Paper presented at the 2007 IEEE Conference on Technologies for Homeland Security: Enhancing Critical Infrastructure Dependability.

Leong, L. H., & Marthandan, G. (2011). *Factors Influencing the Success of the Disaster Recovery Planning Process: A Conceptual Paper.* Paper presented at the International Conference on Research and Innovation in Information Systems, Malaysia, Kuala Lumpur.

Leong, L. H., & Marthandan, G. (2013). Enablers of Successful Business Continuity Management Process. *Australian Journal of Basic and Applied Sciences, 7*(10), 86–97.

Lin, H.-F., & Lin, S.-M. (2008). Determinants of implementation success of e-business systems: using a technology-organization-environment framework. *Technovation, 28*(3), 11.

Linas, M., Arnaud, G., Gunn-Kristin, K., & Terje, O. (2008). Converged service continuity: A challenge for the merchant and the architect. *Bell Lab. Tech. J., 13*(2), 185–192. http://dx.doi.org/10.1002/bltj.20313

Ling, C. (1997). Technology Issues: Sites Built to Battle Computer Disaster–Companies Design Recovery Centers To Keep Data Systems Operating. *Asian Wall Street Journal, 9*.

Lippert, S. K., & Govindarajulu, C. (2006). Technological, Organizational, and Environmental Antecedents to Web Services Adoption. *Communications of the IIMA, 6*(1).

Loftness, S., & Drapeau, M. (2007). What's Missing From Your DR Plan? *Contingency Planning & Management Global Assurance, 4*(6), 12–15.

Mainline Information System. (2006). Ensuring Business Continuity.

McClelland, D. (1973). Testing for competence rather than intelligence.

McClelland, D., & Boyatzis, R. E. (1980). Opportunities for Counselors from the Competency Assessment Movement. *Personnel & Guidance Journal, 58*(5), 368. http://dx.doi.org/10.1002/j.2164-4918.1980.tb00415.x

Menkus, B. (1988). Getting started in data processing disaster recovery. *Computers & Security, 7*(1), 47–52. http://dx.doi.org/10.1016/0167-4048(88)90502-0

Mercury. (2004). *ITIL Best Practices: Maximizing The Business Value of IT - Part II*: Mercury.

Mitroff, I. (2005). Crisis Leadership. *Leadership Excellence, 22*(10), 11.

Mitroff, I. I., & Pauchant, T. C. (1990). Corporations That Prepare for Disaster. *Business & Society Review (00453609)*(75).

OGC Official Site. (2008). Service Management-ITIL® Version 3 Retrieved 100401, 2010, from http://www.best-management-practice.com/Online-Bookshop/IT-Service-Management-ITIL/ITIL-Version-3/

OGC 's Authorized Authors. (2001). *Service Delivery*: OGC ITIL Publications.

Oke, A., Burke, G., & Myers, A. (2007). Innovation Types and Performance in Growing UK SMEs. *International Journal of Operations & Production Management, 27*(7). http://dx.doi.org/10.1108/01443570710756974

Oliveira, T., & Martins, M. F. (2010). Firms Patterns of e-Business Adoption: Evidence for the European Union-27. *Electronic Journal Information Systems Evaluation, 13*(1).

Peter, R. M. (2003). Benefits of Involving Users in Service Innovation. *European Journal of Innovation Management, 6*(4).

Petroni, A. (1999). Managing Information System's Contingencies in Banks: a Case Study. *Disaster Prevention and Management, 8*(2). http://dx.doi.org/10.1108/09653569910266139

Phoommhiphat, M. (2011). *Innovation Adoption in Thai SMEs.* RMIT University.

Pink Elephant. (2006). *The Benefits of ITIL White Paper* (White Paper).

Quarantelli, E. L. (1999). Disaster Related Social Behaviour: Summary of 50 Years of Research Findings. *DRC Preliminary Paper, #280.*

Raj, C. (2008, 2008 July 16). Of technical glitches & conspiracy theories. *Malaysian Business.*

Ramdani, B., Kawalek, P., & Lorenzo, O. (2009). Predicting SMEs' adoption of enterprise systems. *Journal of Enterprise Information Management, 22*(1).

Rogers, E. M. (1995). *Diffusion of Innovation Theory* (4th ed.). New York, Free Press.

Sarif, E. (2008). Technical glitch holds up trading again. *The Star.* Retrieved from http://biz.thestar.com.my/news/story.asp?file=/2008/12/25/business/2891674&sec=business

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for Business Students* (5th ed.). Prentice Hall.

Scott Ream. (2002a). How Does Your Company Measure Up? The Business Continuity Management (BCM) Maturity Model.

Scott Ream. (2002b). How Mature Is Your Business Continuity Program?

Sekaran, U. (2003). *Research Methods for Business.* New York, NY: John Wiley and Sons Inc.

Serrelis, E., & Alexandris, N. (2007). *From High Availability Systems to Fault Tolerant Production Infrastructures.* Paper presented at the Networking and Services. ICNS. Third International Conference on.

Shrivastava, A. K., Payal, N., Kumar, A., & Tiwari, A. (2012). Business Contingency Planning: A Road Map to Protect Company from Unforeseen Threats. *International Journal of Engineering and Advanced Technology, 1*(6).

Skulmoski, G. (2001). Project maturity and competence interface. *Cost Engineering, 43*(6), 11.

SunGuard. (2011). A brief history-from disaster recovery through business continuity to Information Availability.

Tabachnick, B. G., & Fidell, L. S. (2001). *Using Multivariate Statistics* (4th ed.). MA: Allyn & Bacon.

Teo, T. S. H., Lin, S., & Lai, K. H. (2009). Adopters and non-adopters of e-procurement in Singapore: An empirical study. *Omega, 37*(5), 972–987. http://dx.doi.org/10.1016/j.omega.2008.11.001

Teo, T., Tan, M., & Wong, K. (1998). A contingency model of internet adoption in Singapore. *International Journal of Electronic Commerce, 2*(2), 95–118.

The Star. (2006). Hong Leong Bank trying to fix computer glitch. *The Star.*

Thong, J. Y. L. (1999). An integrated model of information systems adoption in small business. *Journal of Management Information Systems, 15*(4), 187–214.

Toigo, W. J. (1996). *Disaster Recovery Planning For Computers and Communication Resources.* John Wiley & Sons, Inc.

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation.* Lexinton MA.

Virgona, T. (2010). *911 2001-A Historical Study of the Human Aspects of Disaster Recovery.* Paper presented at the Proceedings of the Northeast Business & Economics Association.

Voas, J., & Wilbanks, L. (2008). Information and Quality Assurance: An Unsolved, Perpetual Problem for Past and Future Generations. *IT Professional, 10*(3), 10–13. http://dx.doi.org/10.1109/MITP.2008.50

Wadekar, M. (2007). *Enhanced Ethernet for Data Center: Reliable, Channelized and Robust.* Paper presented at the Local & Metropolitan Area Networks, 2007. LANMAN 2007. 15th IEEE Workshop on.

Wang, Y. M., Wang, Y. S., & Yang, Y. F. (2010). Understanding the determinants of RFID adoption in the manufacturing industry. *Technological Forecasting and Social Change, 77*(5). http://dx.doi.org/10.1016/j.techfore.2010.03.006

Wiboonrat, M. (2008). *An Empirical Study on Data Center System Failure Diagnosis.* Paper presented at the

Internet Monitoring and Protection, 2008. ICIMP '08. The Third International Conference on.

Wood, M. (2006). Continuity Planning & Disaster Recovery: ITIL Style.

Woodman, P. (2008). *Business Conitnuity Management 2008 Survey*.

Yang, B. C., Wu, B. E., Shu, P. G., & Yang, M. H. (2006). On establishing the core competency identifying model: A value-activity and process oriented approach. *Industrial Management + Data Systems, 106*(1/2), 60.

Zhongming, W. (2005). Organizational Effectiveness through Technology Innovation and HRM Strategies. *International Journal of Manpower, 26*(6).

Zhu, K., Kraemer, K. L., & Xu, S. (2005). Electronic business adoption by European firms: a cross-country assessment of the facilitators and inhibilators. *European Journal of Information Systems, 12*(4), 251–268. http://dx.doi.org/10.1057/palgrave.ejis.3000475

Zhu, K., Xu, S., & Dedrick, J. (2003). *Assessing Drivers of e-Business value: Results of a Cross-Country Study*. Paper presented at the International Conference on Information Systems.