December 2007

Business Continuity Preparedness and the Mindfulness State of Mind

Tiffany Braun  
Northern Kentucky University

Ben Martz  
Northern Kentucky University

Follow this and additional works at: http://aisel.aisnet.org/amcis2007

Recommended Citation  
http://aisel.aisnet.org/amcis2007/302

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
BUSINESS CONTINUITY PREPAREDNESS AND THE MINDFULNESS STATE OF MIND

Tiffany L. Braun
Northern Kentucky University
braunt2@nku.edu

William Benjamin Martz Jr.
Northern Kentucky University
martzw1@nku.edu

Abstract

Today, with the growing dependence on technology and increasing population growth, the impact of man-made and natural disasters, on human lives and financial losses, is greater than ever. Though some businesses are investing in business continuity planning, others are still reluctant. “An estimated 80 percent of companies without a well-conceived and tested business continuity plan, go out of business within two years of a major disaster” (Santangelo 2004). In this study, we explore why firms in the financial services industry make varying decisions for business continuity planning. Our focus is on business continuity planning for information technology in which we investigate the state of mind of chief executives, within organizations. By applying mindfulness / mindlessness cognitive processes and decision making theories, we attempt to provide insights into what conditions obstruct mindfulness in business continuity planning.

Keywords
Decision making, Organizational Mindfulness and Mindlessness, Business Continuity Planning Preparedness, Disasters

Introduction

Multiple hurricanes, earthquakes, tsunamis, electrical blackouts, flu outbreaks, and global terrorism have increased the level of concern, worldwide, about disasters. Of more concern is that, despite these highly publicized incidents, companies continue to lack fundamentally sound practices, when it comes to dealing with disasters or disruptive events. This is not to imply, however, that all companies are deficient in preparing for disasters. To the contrary, there has been growing interest in the United States, in planning for the unexpected, since the 1993 World Trade Center (WTC) bombings, the Y2K scare of the so-called “millennium bug”, and the September 11th terrorist attacks. Though the WTC bombings and Y2K introduced the need to prepare for unforeseen events, 9/11 brought the need, for business continuity and disaster recovery planning, to the forefront for many companies, especially those who experienced the aforementioned incidents first hand. When the WTC was bombed in 1993, some companies started to question, “What would we do in the event of a disaster?” As a result, businesses started putting together business continuity and disaster recovery plans. For these businesses, when the terrorist attacks hit on September 11, 2001, they were better prepared for evacuating their employees and recovering their business, though they did not anticipate the magnitude of 9/11, which resulted in the loss of many basic services like electricity. Interestingly, these businesses did not anticipate that their backup sites would need to be far enough away to ensure that they were not in the same electrical grid or that the city’s infrastructure would suffer severe damage. They just assumed that any disaster would be limited to a single building, not the entire block or city. The financial services industry was impacted especially hard during 9/11. It was essentially brought to its knees, according to an official from the Security Exchange Commission (SEC) who stated:

“Critical interdependencies of the New York City infrastructure resulted in a disruption of operations for many distant companies, not to mention the financial system vulnerabilities that were exposed. Some back-up facilities were too close
to primary facilities and were disrupted and/or inaccessible. Other facilities were inadequate lacking critical equipment and single points of failure resulted in failed back-up communications system” (Gadziala 2003)

Yet, the financial industry was not alone in their struggles. Many companies, who were effected by 9/11’s disruptions, had inadequate equipment and failed back-up systems. They simply were not prepared. The results of a survey conducted by Infocon Magazine, of CEO’s across the country, in 2003, determined that: “81% of their company’s business continuity plans would not have held up during a catastrophic event similar to the 9/11 attacks” (Naef 2003).

This was the case for the New Orleans City Technical Chief, Greg Meffert, who experienced the inadequacies of his business continuity plan first hand, when Hurricane Katrina hit rupturing the levees. New Orleans found itself to be a city under water and Meffert was left scrambling to rebuild communications (Carr 2006). He was not alone. Many others in New Orleans were also not prepared for this level of catastrophe. As with New York, before 9/11, the companies in New Orleans just did not believe that the threat of a major disaster was imminent, even though there were predictions that a hurricane the size of Katrina would hit New Orleans.

“Approximately 1 out of 4 companies do not have business continuity or disaster recovery plans. Even for companies that have them, almost 20 percent have not been tested in the five years. An estimated 80 percent of companies without a well-conceived and tested business continuity plan go out of business within two years of a major disaster” (Santangelo 2004).

Today, New Orleans is still cleaning up the mess. For some companies, the loss was too great and they will never re-open their doors. According to the Info Security News Magazine (2000), an effective BCP and disaster recovery plan can reduce losses by 90%, when a disaster hits (Naef 2003).

This qualitative work in progress study is looking at the factors that lead to varying levels of business continuity planning (BCP) preparedness. Our focus is on Information Technology (IT) in the financial services industry, due to the BCP regulations required by their governing bodies. We are in the process of interviewing Information Technology Managers, Chief Executive Officers, Chief Information Officers, Chief Financial Officers, and Chief Technical Officers otherwise known as “C” level executives to better understand their state of mind when making decisions that affect BCP preparedness. We will first look at management’s perceived value of IT, how it is leveraged, and related company dependencies. Next, we will introduce the mindfulness and mindlessness cognitive processes in valuing, leveraging and depending in IT. Finally we will ascertain from our data collection if there is a correlation between the level of BCP preparedness and cognitive processes of organizations.

Background

The purpose of a business continuity plan (BCP) or disaster recovery plan (DRP) is to provide procedures, for sustaining essential business operations, during a significant disruption in the business. BCP is mainly focused on the continuation of the business processes, regardless of the size or time of the outage (Whitman et. al 2004). “As long as the organization has time and money at its disposal, the organization can continue to function. Money can take the form of capital, credit lines, investors and the payments from customers” (Cannon et. al 2006). Disaster recovery, often used interchangeably with BCP, is defined as the rebuilding and recovery, after a disaster (Cannon et. al 2006). Business continuity (BC) and disaster recovery (DR) planning have been part of risk management for years. However, prior to 9/11, the planning was focused mainly on local disasters, that is, on single incidents that only impact a building, in which they wanted to protect employees in the event of a building fire or tornado. Today, the scope is much larger, especially after 9/11 and Hurricane Katrina. Now companies should consider that they could lose all services locally, requiring the transfer of their business functions to a facility in another city.

“Katrina opened our eyes to the fact that our business depended on a single facility. We never thought there would be a storm that would take out both facilities – New Orleans and Long Breach,” said Oreck president and CEO, who was referring to his company’s New Orleans and Long Beach, Mississippi manufacturing plants located within 76 miles of each other (Gibson 2006).

One of the residuals from 9/11, when the financial industry in New York was shutdown, was the Government pulling together the Security Exchange Commission (SEC), the Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), Federal Reserve Bank (FRB), the National Credit Union Administration (NCUA), and the Federal Financial Examination Institution Council (FDIC) to create business continuity guidelines. Published in March of 2003, these regulatory guidelines emphasized the critical role that financial institutions play in the economic stability of the United States.
"Financial institutions should recognize their role in supporting systemic financial market business processes (i.e., inter-bank payment systems, and key market clearance and settlement activities) and that service disruptions at their institution may significantly affect the integrity of key financial market" (FFIEC 2003).

The FFIEC, however, was not the only governing body that has published guidelines requiring business continuity planning. Within the financial sector alone, beginning in 1989, the Expedited Funds Availability Act (EFA) was passed stating that the financial services industry must guarantee access to financial resources, during a disaster. Four years later, in 2003, both the Basel II, Basel Committee on Banking Supervision, Sound Practices for Management and Supervision and the Interagency Paper on Sound Practices, to strengthen the resilience of the US financial system, developed their own guidelines for BCP / DRP, with the Interagency Paper requiring BCP upgrades and testing, based on the identified disaster-related risks from the terrorism attacks on the World Trade Center on September 11, 2001 (Noakes-Fry et. al 2005).

With clearly defined regulatory requirements in place since 2003, the question remains why organizations in the financial services industry are reluctant to implement business continuity disaster or recovery plans. Could it be that the financial service-related industries are only recently beginning to feel pressure, to implement business continuity plans, from their regulators? Do these organizations lack the realization that the financial services industry has become increasingly dependent on Information Technology?

Conceptually, business continuity and disaster recovery planning should be a company-wide effort, yet many firms perceive that the responsibility resides in their IT departments. In the financial sector, this perception is not without merit. For financial institutions, who are governed by the FDIC, the regulations addressing business continuity planning are listed in the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook and audited by the IT Audit examiners. This may be due to the fact that most businesses rely heavily on IT for daily operations, a competitive advantage, and to define and execute future business strategies. For example, banks are feeling pressured by their competitors to offer services such as online banking, ATM machines, and real-time deposits and withdraws. They can no longer rely on manual processes and paper copies. Instead, they are forced to use technology to provide fluid and dynamic ways to conduct business, thus challenging and changing the traditional business rules. Since technology is ubiquitous (Haag et. al 2007), institutions have allowed it to become an integral part of the business, thus creating IT dependencies. As a result, any system disruptions may paralyze a company’s ability to make its products, deliver its services, and/or connect with its customers. If the outage extended beyond a few hours, it could significant impact the business. This is especially true for companies who rely on real-time information, such as the eBay or Amazon and whose critical functions depend exclusively on system availability. The loss of profit from unavailable systems would be detrimental. With this increased IT dependency and impact on core operations, why are many companies still reluctant to invest in business continuity planning?

Theoretical Foundation and Conceptual Model

In this section, we discuss the business value of information technology (IT), how it is being leveraged, and its’ increased dependencies. We next introduce mindfulness / mindlessness cognitive processes and decision making theories, to explain why business continuity preparedness, in the financial services industry, varies.

Information Technology

Information Technology is where people use computer based tools to work with information. Haag, Cummings and Phillips, in their Management of Information Systems book, discuss the criticality of information in doing business today. They talk about living in the information age, where knowledge is power. They define knowledge as a combination of information, people, and information technology (Haag et. al 2007). For many businesses, information technology has become their core enabler and way of conducting business (Carr 2003) and (Applegate et. al 2006). Businesses are also looking to leverage information systems to expand into different markets and create competitive advantages. As companies continue to invest in expandable infrastructures, value-add, and value-sustaining applications, they are not only maintaining their profit share, but growing their business (Applegate et. al 2006).

As the use of Information technology (IT) and value becomes omnipresent, so does the dependency. Many businesses have already felt the pain from unavailable systems, especially those impacted by 9/11 and Katrina. Warren F. McFarlan addresses the dependency on IT, in his strategic grid, by showing the impact of IT on businesses. He defines and categorizes IT into four distinct quadrants: support, turnaround, factory, and strategic. He identifies those businesses that reside in the factory quadrant as companies whose existence relies exclusively on IT or those that must have real-time information. Take NASDAQ, for example, can you imagine the cost per minute for system down time? “If the Stock Market was unavailable for more than a few seconds, it could bring the entire [financial] security industry to its knees” (Applegate et. al 2006).
If we apply McFarland’s strategic grid to the financial services industry, most companies within that industry would reside in the factory quadrant. More specifically, if we were to use banks as our example, many are setup using information systems for processing all transactions including deposits, withdraws, payments, online banking, and ATMs. Knowing the potential impact and cost of a bank system outage, one would conjecture that any company residing in the factory quadrant (high IT dependency) would be extremely concerned about backup requirements, disaster recovery, and business continuity planning. If the correlation between impact and level of BCP preparedness is not directly related, what factors influence BCP decision making within these companies?

**Decision Making**

Most individuals want to make the right decisions in every situation. Unfortunately, we are frequently subject to environmental situations or past experiences that may alter our decision making perspectives. Kahneman and Tversky, in their decision making research, have conjectured that decisions are based on our own point of reference and personal experiences (Kahneman et. al 1982). If this is true, then executives with disaster experience, directly or indirectly, should be more open to business continuity planning versus those who have not.

Langer (1975), however, sees decision making differently. She defines it as a phenomenon called “illusion of control” where individuals adjust their decisions based on their perceived impact (Langer 1975). This perception could result in less desirable business continuity decisions. An example of this is where company employees are supportive of BCP, because they see it as protecting their livelihood, yet executives do not see the value. The managers and executives may believe that if a tornado demolishes their facility, they would just move the operation to another location. In this case, the middle manager would be inhibited by his decision making based on his boss’s position.

Another decision making factor that could impact the level of BCP preparedness, is the perceived risk of uncertain situations or events. In the economic theory, risk refers to both gains and losses. Typically, risk perceptions are related to fear and losses, because they are associated with a tragic events or situations, occurring in the future (Klinke 2002). As discussed in the aforementioned section, individuals base their decisions on their own point of reference (Kahneman et. al 1982). If the probability / likelihood of a disaster occurring and any related impact is perceived as low, then the manager will not be willing to invest. If, however, the likelihood of a disaster occurring is high, then we would anticipate a higher level of BCP preparedness, yet this is not always the case.

What about the cost benefit analysis of decisions making? Typically executives and managers make financial-related decisions based on cost benefit analysis. They weigh the costs of developing and maintaining a business continuity plan (BCP) against the benefits or return (Rodewald 2005). For BCP projects, this analysis is flawed since the costs and benefits associated with these projects cannot be quantified (Greer 2001). The BCP output or deliverable reduces or mitigates the impact of disaster, yet there is nothing tangible to measure. BCP is like an insurance policy that will reduce costs in the future.

Though all of these decision making theories seem plausible, a more appropriate framework to evaluate the level of BCP preparedness may be found in the mindfulness and mindlessness cognitive theories.

**Mindfulness and Mindlessness**

One theory, offered by Karl E. Weick, posits why organizations make certain decisions. He classifies management’s decisions as either mindful or mindless. Companies making “mindful decisions make decisions based on reasoning grounded in their own organizational facts and specifics” (Swanson et. al 2004). It is an openness to novelty, alertness to distinction, sensitivity to different contexts, implicit, if not explicit, awareness of multiple perspectives, and an orientation in the present (Sternberg 2000). Weick and Sutcliffe, who studied mindfulness in Highly Reliable Organizations (HRO), define mindfulness as:

“The combination of ongoing scrutiny of existing expectations, continuous refinement and differentiation of expectations based on newer experiences, willingness and capability to invent new expectations that make sense of unprecedented events, and more nuanced appreciation of context and ways to deal with it, and identification of new dimensions of context that improve foresight and current functioning” (Weick 2001).

Their study explored how to manage the unexpected in HRO. They choose HRO due to their success in operating under very stressful conditions. They identified that the significant differences in how HRO and non-HRO reacted to unexpected
circumstances involved the initial identification and response to symptoms and weak signals. “Good management of the unexpected is “mindful” management of the unexpected” (Weick 2001).

Weick and Sutcliffe identified five cognitive dimensions that make up mindfulness: preoccupation with failure or mistakes, reluctance to simplify interpretations, sensitivity to operations, a commitment to resilience, and deference to expertise (Weick 2001).

Preoccupation with failure or mistakes means that decision makers within organizations are constantly looking for failures, regardless of size and seriousness, as symptoms to a larger problem. They treat any irregularity, or slight disruption, as a symptom that something is wrong, possibly resulting in severe consequences. They support and reward individuals who identify errors, then analyze them to make improvements and prevent future occurrences. They are suspicious of potential liabilities related to ongoing success, and are especially concerned with complacency, temptations to reduce margins of safety, and automatic processing. They treat any unplanned changes as if something has gone wrong and could become catastrophic (Weick 2001).

Sensitivity to operations, the second dimension of mindfulness, is when management has a granular understanding of all aspects of the business, both operationally and strategically. They are constantly looking for ambiguity or problems, within their workflows and processes, which may result in a failure. The closely analyze routine tests to reveal any potential or real failures, which might result in an unexpected disaster. They are cognizant of all operations and have a well-developed situational awareness, enabling them to continuously make adjustments to prevent errors. They look for any anomalies, allowing them to be isolated, analyzed, and contained. Their business sensitivity promotes attentiveness to operations and the perception that failures are considered successes. It is an environment in which imperfections and error reporting is encouraged. Individuals are rewarded for questioning and testing assumptions, to find mistakes and errors. Near misses are evidence of successes. Their goal is to ensure ongoing communication among all organizational layers, while clearly defining and valuing each individual layer (Weick 2001).

Reluctance to simplify interpretations, or to accept simplifications, is the third mindfulness dimension. This involves taking clear steps to avoid making things easier or over simplifying the daily operations. Mindful companies situate themselves to see as much as possible, even though the world is a complex, unstable, and unpredictable place. They do not want to restrict or limit their opinion or view, in any way. They promote employees with diverse backgrounds and encourage them to have skepticism, criticism, and push the boundaries for acquiring knowledge, while utilizing careful tactics that will resolve any differences of opinion, without destroying the nuances that diverse people identify. All employees must pay close attention to business operations, with the expectation of avoiding over simplification (Weick 2001).

Finding the most qualified individual to make a decision or complete a job is the fourth dimension of mindfulness. Weick calls this deference to expertise, but it is simply finding the best man for the job and knowing when to escalate the issue him. Mindful organizations have the hierarchal structure that not only recognizes when decisions need to by made by the most qualified individual, but has the capacity to differentiate between low, medium, and high volume times and appropriately escalate emergency situations (Weick 2001).

Commitment to resilience (toughness) is the fifth mindfulness dimension. This is to be mindful of errors and correct them before they get worse. It is anticipating problems and coming up with resolutions, before they occur. Resilience is the ability to quickly recovery when disasters strike (Weick 2001).

“Operating disruptions can occur with or without warning, and the results may be predictable or unknown. Because financial institutions play a crucial role in the United States economy, it is important their business operations are resilient and the effects of disruptions in service are minimized in order to maintain public trust and confidence in our financial system. Effective business continuity planning establishes the basis for financial institutions to maintain and recover business processes when operations have been disrupted unexpectedly” (FFIEC 2003).

Figure 1.  **IT Value and Dependency, in the Organizational State of Mind for Business Continuity Planning Preparedness**
Collective Mindfulness

Proposition 1.1: Collective Mindfulness Increases the Level of Preparedness for Business Continuity Planning

Mindfulness can also be seen in organizations, in which collectively the individuals work together, to synergize expertise. Weick and Roberts define the concept of the collective mind or collective mindfulness “as a pattern of heedful interrelation of action in a social system is the collective mental processes of individuals within an organization or situation” (Weick 1993). Also known as the “group mind,” it is where decisions result from the collective mental processes of individuals within an organization.

Mindfulness in Decision Dynamics

Proposition 1.2: Mindfulness in Decision Dynamics Increases the Level of Preparedness for Business Continuity Planning

Constructs in the decision making literature look to three areas: accountability, routine versus non-routine and environmental characteristics (Roberts et al 1994). Those who are accountable are ultimately responsible for their decisions. These accountable individuals are most likely going to be very mindful in their actions. If they decide not invest in BCP, then they will have a good justification for their actions, especially if their decision impacts human lives. In considering routine versus non-routine decisions, mindful individuals will have the capacity to adjust their decisions. Most disasters, even if the company is mindful in their planning, will require non-routine decisions. With regard to environmental characteristics they can influence decisions due to their complexity and multiple layers. A mindful decision maker in a complex environment must be cognizant of all the varying factors.

Next, we look to the opposite of mindfulness within organizations. We consider three mindless constructs: mindlessness in organizations, groupthink, and the bandwagon phenomena.

Mindlessness

Mindlessness, on the other hand, is the logical inverse of mindfulness. Weick et al defines a mindless firm as: "One that takes actions that betray an absence of such attention and grounding” (Weick et al 1999). Mindlessness is the undertaking of activities that follows a set recipe without question, uses old categories or standard operating procedures, utilizes rigid and inflexible decisions and thought processes, and does not easily identify problems. Mindlessness is like continuing to fly an airplane on autopilot, without questioning its accuracy, even though you continue to fly off course. It is an individual lack of awareness and sensitivity to the business. It is the transfer of blame, denial, and / or a lack of understanding. It is characterized by a preoccupation with success and a denial of failures. Top management either ignores, or is shielded from, bad news. Mindless management rarely looks for failures, believing that none will be found. They allow slowdowns to be underreported and incubated until they are almost undeniable and irreversible. Mindless firms often make decisions based on the bandwagon or the “me too” phenomena (Fiol 2003).

The premise of Mindlessness most recently was demonstrated in an article from Computerworld Magazine. They conducted a survey of CIO’s and asked what they perceived the possibility of a major bird flu pandemic outbreak to be and what impact it would have on their operations. Overwhelmingly, most stated that it isn’t that big of a concern for them: “I don’t view the
pandemic preparations as that important,” said Amy Fowler, president of Colorado chapter of Society for Information Management and an IT management consultant for large companies (Hamblen 2006).

**Mindlessness in Groupthink**

*Proposition 2. 1: Mindlessness in Groupthink decreases the Level of Preparedness for Business Continuity Planning*

Another more documented instance of mindlessness is a group dysfunction known as GroupThink. Griffen (1997) defines GroupThink as “a mode of thinking that people engage in when they are deeply involved in a cohesive in-group, when the members’ strivings for unanimity override their motivation to realistically appraise alternative courses of action” (Griffin 1997). Though not all aspects of this theory apply to mindless, several aspects demonstrate similar traits. For example, the Groupthink characteristic called “illusion of invulnerability” is where mindlessness is demonstrated by companies developing, a false sense of security in respect to disasters. As mentioned in the introduction, this type of mindlessness was apparent during hurricane Katrina. The second characteristic of Groupthink that is applicable is the belief in inherit morality of the group or a righteous belief. Once again an impervious attitude that is a mindless behavior. “Everybody operated on the notion that you would leave during a hurricane for two or three days and then come back. Shutting down the data center, backing up the tapes – everything would work just fine. But nobody contemplated the impact. It was regional.” said Barron, interim provost vice president for IT and the CIO of Tulane, in New Orleans (Gibson 2006).

**Bandwagon Phenomena**

*Proposition 2. 2: Mindless Bandwagon Phenomena decreases the Level of Preparedness for Business Continuity Planning*

The mindlessness phenomena, known as bandwagon, is the process in which an individual or an organization adopts an idea, technology, product, or way of doing things based on the number of others who have already adopted it, without their own investigation (Fiol 2003). It is the “me too” phenomena that becomes routine for many organization. They either do not want to spend the time or money to mindfully make the decision. They rely on others for their decisions.

![Figure 2. Perception of Information Technology Value and the Level of Mindfulness in Business Operations](image)

**Exploratory Fieldwork Study**

In the context of business continuity planning, we are conducting exploratory interviews with management and executives from the financial services industry. From our interviews, we hope to better understand and explain the varying levels of IT-related business continuity planning preparedness. Our questions are derived from the “mindfulness/mindlessness” framework, of Karl E. Weick, to help determine whether management’s mindset influences the varying levels of BCP preparedness. We will consider how the level of mindfulness, in business operations, directly corresponds to management’s perception of information technology’s value and dependence on the business.
Conclusion and Future Impact

In summary, we conjecture that decision making theories as well as the mindfulness and mindlessness cognitive processes impact the level of business continuity preparedness in organizations. This organizational state of mind and inhibited decision making, coupled with the perceived value and dependency on information technology, appears to have a direct relationship with the level of BCP preparedness, in financial institutions. By understanding the factors that contribute to mindfulness and mindlessness cognitive processes and decision making theories, as it relates to BCP preparedness, management, executives, regulators, and auditors will have new insight for reducing the economic impact of unexpected disasters. This insight could result in assisting businesses and the BCP community in building a set of “Lessons Learned” for BCP.

Figure 3. Business Continuity Preparedness, the Perception of Information Technology Value, and the Level of Mindfulness in Business Operations
References


Santangelo, V. (2004) "Many business are unprepared to survive disaster." Puget Sound Business Journal (Seattle) Volume, DOI:


