3-1-2007

Disaster Recovery Practices in Small Business: A Delphi Study of Factors Affecting Adoption

Barry A. Cumbie
cumbiba@auburn.edu

DISASTER RECOVERY PRACTICES IN SMALL BUSINESS: A DELPHI STUDY OF FACTORS AFFECTING ADOPTION

Barry A. Cumbie
Auburn University
cumbiba@auburn.edu

Abstract

In response to the devastation of recent hurricanes in the Gulf Coast, this research in progress intends to identify small businesses that are at-risk of failing if they experience a data loss caused by a community-wide natural disaster. As guided by classical innovation diffusion theory, the phenomenon of adopting disaster recovery practices within small businesses is studied form the point-of-view of small businesses. Practitioner-oriented literature is reviewed to identify relevant disaster recovery practices that are classified within a risk management framework. A Delphi study is initiated among small businesses to (a) identify current disaster recovery practices employed to prevent data loss, and (b) ascertain the current levels of awareness and adoption of disaster recovery practices. The results of the review are reported along with the initial findings of a Delphi study still in progress.

Keywords: Small Business, Disaster Recovery, Delphi Study, Innovation Diffusion

Introduction

In 2005, Hurricanes Katrina and Rita devastated the Gulf Coast, the repercussions are still being felt today. Forecasts predict future hurricane seasons being more active (Loney, 2006), begging the question of how to assuage loss caused by future storms. Poignant in the MIS domain are concerns of how organizations manage data and information systems (IS). In light of recent disasters, this study's focus is on the adoption of disaster recovery practices related to organizational data and IS.

Small businesses are critical in the US economy as well as economies of all nations (Carland, Hoy, Boulton, & Carland, 1984; Nooteboom, 1988; Palvia, 1996), yet they are most vulnerable to failure after a disaster (Stephens, 2003). Additionally, significant data loss contributes to business failure (Rike, 2003). Thus, a disaster such as a Gulf Coast hurricane likely contributes to small business failure but may be curbed if data loss is mitigated.

A Delphi study is initiated among small businesses owners primarily in Alabama's storm-prone Gulf Coast to accomplish the following: (a) identify current disaster recovery practices employed to prevent data loss, and (b) ascertain the current levels of awareness and adoption of disaster recovery practices. These efforts intend to serve as groundwork for future research, specifically action research studies aimed at increasing the rate of adoption of disaster recovery practices as informed by the theoretical perspective of innovation diffusion. This study also intends to avoid pitfalls of haphazardly invoking models of innovation diffusion by first identifying and understanding the needs of the target population from a local viewpoint (Rogers, 2003). A risk analysis framework is adopted to guide a review of disaster recovery. The next section presents the theoretical background, which is followed by a concise summary of a literature review of disaster recovery. Following the review summary, the research method used for this study is presented and the initial findings are reported. This paper concludes with tentative findings and research contributions.

Theoretical Background: Precursor to Innovation Diffusion

Three key statistics drive this study: 43% of businesses fail immediately after disaster (Wenk, 2004), 93% fail after significant data loss (Rike, 2003), and 65% of small- and medium-sized firms do not have a disaster recovery plan (Gartner, 2002). Given the high rates of failure and the high rate of non-adoption, which includes small businesses, a comprehensive portrait of non-adopters may help understand the decision to not adopt presumably helpful

practices. The theoretical perspective of innovation diffusion identifies variables that contribute to the rate of innovation adoption of including perceived attributes of the innovation, the type of the innovation-decision, communication channels, nature of the social system, and extent of change agent promotion efforts (Rogers, 2003). Innovation diffusion is rooted in action research methods, in which land-grant university extension agents sought to increase adoption rates of improved products and methods among farmers (Rogers).

Several pitfalls inhibit researchers from clearly understanding the phenomena of adoption or non-adoption of any innovation (Rogers, 2003). A pro-innovation bias is one in which researchers and other experts assume that an innovation – disaster recovery – ought to be adopted by everyone within the population – small businesses. Rogers offers several methods to avoid the pro-innovation bias. First, a field experiment in which data are collected at more than one point in time, i.e., before and after a treatment. This research method negates the tendency to study only successfully diffused innovations. Additionally, the selection of the innovation under study should be done with care. Unsuccessful diffusions, or non-adoption choices, should be evaluated from a local viewpoint. As many of the decision factors about an innovation are perceptions, it is important to understand the perception of the innovation from the viewpoint of potential adopters and not from the researcher's.

Disaster recovery is a preventative innovation, or "a new idea that an individual adopts now in order to lower the probability of some unwanted future event" (Rogers, 2003), p. 234). Preventative innovations are contrasted against incremental innovations that are characterized by having near-term, relatively clear-cut outcomes. Preventative innovations have delayed results, injecting uncertainty of favorable outcomes being directly related to the adoption of an innovation. For example, small businesses adopting a disaster recovery plan are only capable of assessing the value of the adoption when and if a disaster ever occurs. Even then, the elapsed time since initially adopting the innovation might obscure any direct association with positive or negative consequences. These barriers are further compounded with the innate nature of data of which value is difficult to assess (Freeman, 2000).

However difficult for small businesses to perceive the value of adopting disaster recovery innovations, they should not necessarily be blamed for non-adoption. The individual-blame bias involves a researcher assigning fault for a behavior among a population under study (Rogers, 2003). To counter this, alternative explanations should be sought including system-blame factors such as the overarching social structure to which the population belongs. Furthermore, establishing empathy is especially critical in the case of preventative innovation in which the target population is at-risk of exposure to a given threat. The Stanford Heart Disease Prevention Program in the 1970's and 1980's exemplify a successful diffusion of preventative innovations such as quitting smoking, exercising, and dietary changes to prevent heart disease (Rogers). Their success hinged not on assigning blame, but identifying high-risk individuals and then directing mass media communications and small group training toward them.

As explored in the following section, knowledge of disaster recovery is expected to be high because of the great deal of attention on this subject by practitioner-oriented literature. Additionally, Hurricane's Katrina and Rita are cue-to-actions in which the threat of a disaster is manifest in a very real way (Rogers, 2003). Despite this attention, the practice of adopting disaster recovery is reportedly low (Gartner, 2002). Heeding the precautions outlined by Rogers, this study focuses on understanding the nature of the disaster recovery innovation from the perspective of the adopters.

Literature Review Summary: Disaster Recovery Practices

Disaster recovery is a component of the broader concept of information security (Greenmeier, 2006). Unfortunately, IS research in information security sparse perhaps because of the intrusiveness of security research and the reluctance of organizations to reveal information about their current state of security to outsiders (Kotulic & Clark, 2004). Reporting weaknesses could unsettle stakeholders or identify areas of exploitation to competitors or hackers. Evidence of the paucity of research in this area is presented by Cumbie (2007).

Perhaps because of the great attention given by the trade press to data preservation and the expertise of numerous software and service providers (e.g., Janusz, 1993; LaPage & Gaylord, 2003; Molina, 1996; Phillips, 1999; Vachon, 2003), academic research has left this topic to the practitioners. The temptation is great to consider disaster recovery practices as commonplace and ignore the organizations that do not have such controls in place. This may be an example of pro-innovation bias and individual-blame bias, two common research fallacies identified by innovation diffusion theory (Rogers, 2003). Recognizing the negative impact of data loss in small businesses caused by disaster and the absence of planning, this study turns to other academic disciplines and the practitioner-oriented literature to build a coherent understanding of disaster recovery. A risk analysis phase from Gibb and Buchanan's (2006)

business continuity framework is used to organize the following review of disaster recovery practices. Within Gibb and Buchanan's risk analysis phase, a risk identification stage categorizes risks and is followed by risk evaluation stage to assess the business impact in the event of a risk.

In lieu of the details of the literature review, a summary of the results are given. IS Threats to data can be classified in one of three disaster categories specified by Rike (2003): human, technical or mechanical, and natural or environmental hazards. Classifying IS threats into categories is useful because the method of preparedness differs depending on the category and locus of impact. The primary distinction of natural threats from all others is the lack of control that can be exercised by human action. For all other types of threats, human intervention can be effective at reducing the likelihood of their occurrence. Natural disasters, however, are furthest beyond the reach of organizations control. The goal of management is to prepare for the impacts, to weather the storm, rather than preventing them outright.

Of the three strategies of risk mitigation – transfer, minimize, or absorb (Gibb & Buchanan, 2006) – minimization is the only viable option for small business response to natural disasters. Transferring risk by insuring against disasters may offset loss of IS, but the data lost cannot be replaced or assigned an accurate monetary value. Outsourcing transfers risks to another party, but control of valuable company information is sacrificed. Absorbing a risk is appropriate when the costs of preparation outweigh the benefits, certainly not the case in light of the high rate of business failure after a disaster. Minimization of risk is the only option to mitigate risks of natural disasters; hence, the focus of disaster recovery practices to prevent data loss. Data and IS systems resources critical to a business must be identified so that a commensurate disaster recovery practice can be enacted.

Consistent with Gibb and Buchanan's (2006) business continuity framework, the next logical step is to select an appropriate disaster recovery practice. Reviewed literature revealed four preconditions that must be met prior to discussing specific disaster recovery practices: practices employed by small businesses in response to natural disasters must be off-site, encrypted, digitized, and compliant with regulatory mandates. On-site solutions do not provide necessary diversity from a threat; encrypted data negates the loss of control of data-in-transit; digitalization is both a precursor to encryption and enables relatively easy duplication, transportation, and storage of data compared to paper-based data; and compliance to mandates such as the Health Insurance Portability and Accountability Act (HIPPA) may be a necessary legal requirement for an industry.

Given the preconditions of practices being off-site, encrypted, digitized, and compliant, the specific practices appropriate for small businesses to mitigate the impact of community-wide disasters are either IS-oriented or data-oriented. IS-oriented practices focus on resuming operations from a hardware and software perspective, ensuring that the proper systems, configurations, licenses, and passwords are in place as needed after a disaster. Data-oriented practices complement IS-oriented practices by providing data to be used by the software and hardware and are either online or external. The practice selected largely depends on the minimum allowable time in which IS or data can remain unavailable before operations cease after incurring a disaster, or the recovery time objective (RTO). The RTO dictates the use of hot- (fully redundant data centers) or cold-sites (computer ready facilities), or the use of mobile recovery units (self-contained computer equipped trailers). Also related to the RTO is the method of data backup which includes the choice of media, rotating media to add diversity, and the nature of the backup (full, incremental, or selective). The grandfather/father/son media rotation practice provides the most resilience to media failure and data loss by rotating the use of four storage media for weekday incremental backups, three storage media for end of the week full backups, and twelve end of the month full backups (Buffington, 1997).

For each disaster recovery practice that satisfies the preconditions, both governance and restoration are post-conditions that are decided upon when selecting a practice. Governance involves whether a selected disaster recovery practice is performed in-house or by a third-party. Third-parties may offer specialized expertise but at the expense of management control and managing relationships. For any practice or mode of governance, a vital but often overlooked component of disaster recovery is testing to ensure that the data and IS are restored properly (Gibb & Buchanan, 2006; Mearian, 2005).

In-house practices fail to achieve geographical diversity, leaving off-site solutions as viable disaster recovery practices. The use and storage of external media follows the same rule of diversity, needing to be routinely rotated. Storage of external media introduces information security vulnerabilities which can be minimized with data encryption. The chosen governance mode depends on the level of expertise and desired level of control retained; the use of a service provider transfers responsibility but sacrifices control. Finally, an untested disaster recovery practice is potentially equivalent to no practice at all.

Research Method: Delphi Study

The purpose, guided by Rogers (2003), is to understand disaster recovery from the perspective of potential adopters. Searching the literature does not provide this perspective but is useful to establish an initial understanding of disaster recovery for comparison. The Delphi research method was selected as an effective way to identify and prioritize issues of interest that can both avoid the bias of researchers and capture the local viewpoint of small business managers while allowing the flexibility to delve deeper into the research questions (Okoli & Pawlowski, 2004).

Following the guidelines set by Okoli and Pawlowski (2004) of how to conduct a valid Delphi study, three phases – brainstorming, narrowing down, and ranking – are conducted to identify relevant issues among an assembled panel of experts. The experts respond independently and anonymously from each other while the researcher acts as a liaison to solicit and compile responses, and calculate a statistical measure of consensus, namely Kendall's *W*.

Participants were identified by consulting with chamber of commerce officials in Alabama's Baldwin County, an area prone to hurricanes. The panel was rounded out with two non-coastal, IT companies to provide contrast. Demographics of the participants will be provided upon the completion of the study, yet all can be classified as *very* small business (i.e., those with 100 or fewer employees, Palvia, 1996).

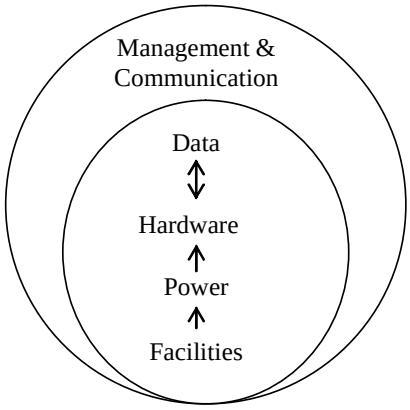

Figure 1. Conceptualization of Disaster Recovery Practices

Initial Findings

The first phase of the study asked participants to respond to the following instruction: list the elements (in no particular order) of disaster recovery practices that are appropriate to secure electronic data from a community-wide natural disaster such as Hurricane Katrina, and (b) list the most important issues (in no particular order) that either encouraged or prohibited your organization from adopting any one disaster recovery practice. Not all responses have been received and Table 1 lists the responses received thus far from eight participants. The categorizations of responses represent an initial attempt by the researcher to develop a framework to classify these practices. Figure 1 conceptualizes the categorization: data and hardware are interdependent, hardware is dependent on a power supply and both depend on facilities to house the hardware. All of this is nested within communication and management, two categories that provide decision making and coordination of all disaster recovery practices. Data are at the core of disaster recovery. Facilities, power supply, and hardware while necessary to access electronic data are far less critical than the data itself. It is unlikely that lost data such as financial records or e-mail messages can be accurately and fully recreated, but a destroyed building or server can be replaced with little consequence to the data.

The issues given for not adopting any one of these practices begin with financial and time restraints: lack of funds to purchase a generator, to remodel facilities to protect servers, time taken from more pressing business matters including daily operations, and lack of technical expertise. Other notable reasons given were no IT staff to exert pressure, high rates of employee turnover, and the complexity of using a patchwork of different solutions.

Table 1. Categorized Results of the Phase 1 of relevant Disaster Recovery Practices

Category	Disaster Recovery Practice
Management (internal)	Perform a risk analysis to identify real threats Ensure technical IT expertise to perform actual practices Ensure business IT expertise to assess value of data Devise a comprehensive recovery plan for daily to large scale emergencies Plan to rebuild servers Plan to restore data Plan for continuous power (electricity preparedness) Plan for continued access to facilities Designate roles and responsibilities Simulate an emergency
Management (external)	Select geographically diverse service providers (e.g. web hosts and data centers) Purchase business disruption insurance Establish a line of credit with a bank to ensure cash flow Prepare a public relations statement to inform the press and public
Communication	Provide remote access to data and e-mail via the Internet Establish a single communication touch-point for employees Establish a toll-free number for employees to update their whereabouts, ability to work, and to learn when to return to work Set up communications alternative to phones and cell phones for contact with vendors and outsourced support Update a website for communication with partners
In-house data	Perform daily backups of server data onto storage media Backup desktop data as needed Store digital media (e.g magnetic tape) off site Store at a nearby facility for fast access Store a geographically diverse location to minimize risk Test restoring data to ensure accuracy Test on alternative hardware
Computer hardware	Locate servers in a secure room Logoff from and shutdown computers Include both desktops and servers Unplug all electronics Move computers away from windows and off the floor Cover unplugged electronic equipment with plastic sheeting Remove hardware from facilities Relocate hardware to a dedicated hosting center
Power	Pre-arrange stand-by power with ample fuel and access to re-supply Charged laptop batteries Use battery backup for hardware
Facilities	Access to facilities (esp. leased, pass/fee for reentry)

Discussion & Conclusion

Upon the conclusion of the Delphi study, it will be interesting to contrast the responses from the expert panel with that of the literature. Together these two sources can contribute to an overall portrait of the relevant practices used among small business and the reasons why some fail to adopt them. At this point, the preeminence of data over other issues such as continued access to facilities or power may help reduce the complexity of the problem; allowing small business managers to focus on protecting their data and only then turning to other matters.

Assuming that adopting disaster recovery practices will help prevent business failure due to data loss is a simplified view. The responses given in the Delphi study should support or refute this simple and linear relationship. If supported, efforts should be given to educating small business managers or to designing disaster recovery practices that lend themselves to easier adoption. If refuted, alternative contributing factors to business failure will need to be addressed.

References

Buffington, J. L. (1997). Today's window of exposure for data loss. *Computer Technology Review, Winter*, 74-81.

Carland, J. W., Hoy, F., Boulton, W. R., & Carland, J. C. (1984). Differentiating entrepreneurs form small business owners: A conceptualization. *Academy of Management Review, 9*(2), 354-359.

Cumbie, B. A. (2007). Disaster reocvyer: An innovation diffusion perspective. *work in progress*.

Freeman, E. Q. (2000). E-merging risks: Operational issues and solutions in a cyberage. *Risk Management, 47*(7), 12-15.

Gartner. (2002). Gartner says most small and midsize businesses are not prepared for a crisis. Retrieved August 2, 2006, from http://www.dataquest.com/press_gartner/quickstats/busContinuity.html

Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management, 26*(2), 128-141.

Greenmeier, L. (2006). No more excuses. *Information Week, 1091*, 23-25.

Janusz, C. (1993). Selecting UPS systems for midrange computers. *Computer Technology Review, 13*(11), 110-112.

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

LaPage, A., & Gaylord, K. (2003). Protect against data loss with W2K's backup utility. *Windows Professional, 8*(2), 8-12.

Loney, J. (2006). US predicts active hurricane season. Retrieved May 22, 2006, from http://today.reuters.com/news/newsarticle.aspx?type=domesticNews&storyid=2006-05-22T152709Z_01_N22385894_RTRUKOC_0_US-WEATHER-HURRICANES-NOAA.xml&src=rss

Mearian, L. (2005). IT managers criticize federal data-loss bill. *Computerworld, 29*(30), 10.

Molina, J. (1996). A RAID status report. *Computer Technology Review, 16*(9), 44-45.

Nooteboom, B. (1988). The facts about small business and the real values of its 'life world': A social philosophical interpretation of this sector of the modern economy. *American Journal of Economics and Sociology, 47*(3), 299-314.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management, 42*(1), 15-29.

Palvia, P. C. (1996). A model and instrument for measuring small business user satisfaction with information technology. *Information & Management, 31*(2), 151-163.

Phillips, J. T. (1999). Will data conversion lose your records? *Information Management Journal, 33*(4), 56-59.

Rike, B. (2003). Prepared or not...That IS the vital question. *Information Management Journal, 37*(3), 25-33.

Rogers, E. M. (2003). *Diffusion of Innovations* (Fifth ed.). New York, NY: Free Press.

Stephens, D. O. (2003). Protecting records in the face of chaos, calamity, and cataclysm. *Information Management Journal, 37*(1), 33-40.

Vachon, L. A. (2003). Recover from a data-loss disaster with GetDataBack. *Windows Professional, 8*(2), 12-14.

Wenk, D. (2004). Is 'Good Enough' storage good enough for compliance? *Disaster Recovery Journal, 17*(11), 1-3.