December 2007

The Essential Components of Disaster Recovery Methods: A Delphi Study Among Small Businesses

Barry Cumbie
Auburn University

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

Recommended Citation
http://aisel.aisnet.org/amcis2007/115

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.
THE ESSENTIAL COMPONENTS OF DISASTER RECOVERY METHODS: A DELPHI STUDY AMONG SMALL BUSINESSES

Barry A. Cumbie
Auburn University
cumbiba@auburn.edu

Abstract

In response to the devastation of recent hurricanes in the Gulf Coast, this research identifies small businesses as being at-risk of failing if they experience a data loss caused by a community-wide natural disaster. Practitioner-oriented literature is reviewed to identify relevant disaster recovery components that are classified within a risk management framework. A Delphi study is conducted among small businesses to identify essential disaster recovery practices employed to prevent data and IS loss. The results of the review along with the findings of a Delphi study are reported and together establish a comprehensive portrait of the essential components of disaster recovery methods for small businesses in response to the threat of community-wide natural disasters.

Keywords: Information Security, Disaster Recovery, Small Business, Community-Wide Natural Disasters, Delphi Study

Introduction

In 2004 Hurricane Ivan wreaked havoc on Alabama’s coastline and the repercussions are still affecting coastal communities as of today. The next year Hurricanes Katrina and Rita swept through the Gulf Coast and future hurricane seasons are predicted to be even more active (Loney, 2006). Among the devastating consequences of these storms is the compromise to information security, a research area that includes the organizational strategies and responses to information systems (IS) threats (Greenmeier, 2006). Upon reviewing many incidents of IS breaches included in the three IS threat categories – human, technical/mechanical, and natural/environmental (Rike, 2003) – a feature that distinguished natural threats from all others is the lack of human control\(^1\). For both human and technical threats, organizational intervention is potentially effective at reducing the likelihood or outrightly preventing their occurrence.

The unexpected occurrence of natural disasters, however, cannot be reasonably prevented and instead requires a strategy of preparedness to minimize the negative effects. Naturally, human or technical threats that result in effects similar to natural threats can be considered together with natural disasters but are beyond the scope of this study. Furthermore, the many types of natural disasters can be distinguished by their geographical range of impact. Community-wide natural disasters – those that impact beyond a wide geographically area, e.g. a hurricane or an earthquake – accompany more
substantial economic loss and widespread infrastructure damage than geographically isolated natural disasters (e.g. a sinkhole). Because of their greater and negative economic impact, this study’s focus is community-wide natural disasters rather than localized ones. Henceforth, the term “disaster recovery methods” or any related phases denote any prophylactic practice related to reducing the likelihood that a community-wide natural disaster will result in unrecoverable losses of electronically stored organizational data and IS.

After a disaster, a reported 43% of businesses never reopen (Wenk, 2004). Compounding this problem is the reported 93% business failure rate following a significant data loss (Rike, 2003). A community-wide natural disaster that affects both the physical and IS aspects of an organization is a threat to the vitality of organizations. Even so, 65% of small- and medium-sized businesses have not devised a disaster recovery plan (Gartner, 2002). The non-adoption of planning among small businesses is not unexpected given the absence of small business organizational characteristics such as long-term planning, specialized staff, decentralized decision making, financial resources, organizational slack, and scale that leads to IS success; together the lack of these characteristics are described as resource poverty (d'Amboise & Muldowney, 1988; Igbaria, Zinatelli, Cragg, & Cavaye, 1997; Thong, 1999).

Despite the obstacles faced by small businesses, trends in information technology (IT) are enabling even the smallest of firms to be not only IT-equipped but also to achieve previously unreachable levels of IT and IS sophistication (Copeland, 2006; Cragg & King, 1993; Delone, 1988; Raymond & Pare, 1992; Thong, 1999; Wailgum, 2006). The extent of organizational resource poverty heightens the vulnerability to loss of organizational data and IS to a community-wide natural disaster. The vulnerable state of small businesses is alarming when their economic role is considered. Small businesses are critical in the United States economy as well as economies of all nations (Carland, Hoy, Boulton, & Carland, 1984; Nooteboom, 1988; Palvia, 1996; Street & Meister, 2004; Thong, 1999). In the U.S. alone, small business comprise 99.7% of all employers and are responsible for nearly half of private jobs, domestic private sales, and private sector output according to the U.S. Small Business Administration.

Because of the reported rates of failure accompanying data loss, increased adoption of IT and IS, increased vulnerability coupled with economic importance, and reported rates of lack of planning, this study attempts to formulate a comprehensive portrait of the essential components of disaster recovery methods applicable to small businesses. A myriad of available strategies and technologies are available from which small business managers can select. The presence of many options contribute to the perceived complexity of these methods which theoretically inhibits their adoption (Davis, 1989; Rogers, 2003). To reduce the complexity of managerial decisions regarding disaster recovery methods, this study seeks to clarify the issue by qualitatively and empirically addressing this research problem from the perspective of small business executives. Furthermore, a thorough investigation of the IT artifact is critical for IS research to understand the characteristics of fast-changing technology and to lend context to research theory (Orlikowski & Iacono, 2001). The administration and
results of a literature review and Delphi research study that lead to a comprehensive portrait of disaster recovery methods are presented in the following sections.

Research Background

A comprehensive understanding of the IT artifact under study is imperative to distinguish the extent to which an organization has adopted disaster recovery methods. Turning first to IS academic literature, components of disaster recovery methods that are appropriate to reduce the likelihood that a community-wide natural disaster will result in unrecoverable losses of electronically stored organizational data and IS are sought. Upon discovering a paucity among IS literature, the same information is sought from practitioner-oriented literature and other academic disciplines. The identified components from the literature review are combined and validated by way of an Delphi study. 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 obtain rich data toward a research questions (Okoli & Pawlowski, 2004).

A search among the top ten IS journals (Mylonopoulos & Theoharakis, 2001) for “disaster recovery” and related terms from the ABI/INFORM database yielded ten results of which only one addressed this topic in a rigorous academic sense. Unfortunately, IS research in information security sparse because of its intrusiveness of studies 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 saboteurs.

Turning to the practitioner-oriented literature, the same search for the term “disaster recovery” yielded over 7,000 results. Of these results, several are guides and tutorials for specific disaster recovery methods while others present statistics and stress the importance of planning for a disaster. Articles were scanned for relevancy and the review was organized by Gibb and Buchanan’s (2006) risk assessment step of a business continuity planning framework. In this manner the range of IS threats, geographical scope, type of data loss, and disaster recovery components were identified and classified. The results of these efforts defined the scope of this study and are reported together with the results of the Delphi study.

Research Method

After a review of practitioner-oriented literature a Delphi study was initiated according to the guidelines set by Okoli and Pawlowski (2004) of how to conduct a valid Delphi study. Three phases – brainstorming, narrowing down, and ranking – were 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
Components of Disaster Recovery Methods, Cumbie

A measure of consensus. Kendall’s $W$ coefficient of concordance is a non-parametric measure of consensus among related samples; a value of 0.7 in a possible range of 0 (no consensus) to 1 (perfect consensus) indicates a satisfactory level of agreement (Okoli & Pawlowski, 2004).

Participants were identified by independent consultations with two county officials in Alabama’s Baldwin County, an area prone to hurricanes. The panel was rounded out with three non-coastal, IT companies to provide contrast. Overall, nine of the twenty recruited executives of small businesses participated throughout all phases of the study while each phase had ten participants, meeting the threshold on generally accepted number of participants (Okoli & Pawlowski, 2004). The demographical information of the participants who participated in all phases is presented in Table 1. The study was conducted from November 8, 2006 until February 27, 2007 and was administered entirely via e-mail. The duration of the study includes a five day recruiting period and suspension of the study over the holiday season.

Table 1
Delphi Study Demographic and Descriptive Statistics†

<table>
<thead>
<tr>
<th>Demographic</th>
<th>Mean</th>
<th>Std. Dev.</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Years in Business</td>
<td>23.9</td>
<td>29.1</td>
<td>[5, 87]</td>
</tr>
<tr>
<td>Years Employed</td>
<td>8.8</td>
<td>6.3</td>
<td>[1.5 22]</td>
</tr>
<tr>
<td>Estimated Number of Employees††</td>
<td>24</td>
<td>33</td>
<td>[1, 95]</td>
</tr>
<tr>
<td>Estimated Revenues (in $1,000)††</td>
<td>2,073</td>
<td>2,205</td>
<td>[25, 5000(+)]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Demographic</th>
<th>Number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privately owned</td>
<td>7</td>
<td>78</td>
</tr>
<tr>
<td>Family owned</td>
<td>3</td>
<td>33</td>
</tr>
<tr>
<td>Centralized</td>
<td>8</td>
<td>89</td>
</tr>
<tr>
<td>Formal IT staff</td>
<td>4</td>
<td>44</td>
</tr>
</tbody>
</table>

† N = 9
†† A conservative estimate calculated from precise and estimated responses

Results

The first of the three phases asked participants to brainstorm about the components of disaster recovery methods that are appropriate to protect against a community-wide natural disaster. Throughout the three phases, participants were able to combine like items, edit existing items, or append new items to the lists. During the brainstorming phase, forty disaster recovery components were identified. The second phase, narrowing down, resulted in ten components that were retained by at least 40% of the participants. Of the ten components three were retained by six participants, two by five participants, and the remaining five by four participants. The third phase involved stack-ranking the components in order of importance.
After one round the group reached a low level of consensus measurement (Kendall’s $W = 0.135$), indicating disagreement in the rankings. Okoli and Pawlowski (2004) suggest that the respondents are asked to re-rank the components until a satisfactory consensus is achieved, Kendall’s $W$ does not significantly improve, or after three rounds. This study departed from suggestions and subsequent re-ranking rounds were not conducted due to the following three reasons: increasing tardiness of responses indicating fatigue among participants, a concurrent Delphi study that was being administered to the same panel had failed to improve during subsequent rounds, and that the disaster recovery methods are considered to be effective when enacted holistically and not piecemeal.

The results of the literature review together with the results of the Delphi study together lead to a comprehensive model of components essential to appropriate disaster recovery methods. The components are classified as either managerial or operational and are presented in a logical sequential order. Managerial components mirror the traditional management functions of controlling, planning, leading, and organizing; these functions establish the guidelines for which operational components are enacted. Operational components refer to the specific details of disaster recovery methods including components that are common to all methods and those that vary according to the maximum allowable time an organization can operate without its data.

**Managerial Control**

The first step toward understanding disaster recovery methods is the managerial action of exerting control of data and IS. A baseline degree of control is established by conducting an analysis of the possibility and impact of a disaster. Small business executives identified the act of performing a risk analysis including the identification of the nature of the threat as one of the most important components of a comprehensive disaster recovery method. A business continuity framework such as the one developed by Gibb and Buchanan (2006) consists of a risk identification phase to categorize risks and is followed by risk evaluation phase to assess the business impact in the event of a risk. To identify the risks to organizational data a broad categorization of threats to organizational IS was reviewed. Identification of threats to IS allows for managerial control to be exercised. Disaster recovery methods that relate to the loss of historic data and ongoing transactional data collection in the face of community-wide natural disasters call for a strategy of preparedness versus prevention.

Evaluating the impact of a realized risk on the business is useful for the effective allocation of resources and follows the risk identification phase of Gibb & Buchanan’s (2006) framework. For many businesses in disaster prone regions such as the U.S. Gulf Coast, the question is not if a hurricane will happen again (Loney, 2006). Determining the impact of a community-wide natural disaster on a small business depends on the value attributed to data an IS. Several authors refer to mission or business critical data (Chouinard, 2003; Essex, 2000; Ferelli, 2001; Hawkins, Yin, & Chou, 2000). Data and IS
resources are critical if in their absence, an organization would soon either suffer irreversible damages that would forever change the organization including the cessation of operations. Critical data and IS resources depend on a specific organization’s industry and business practices. For instance, client-centric organizations as accountant firms and document-centric firms such as publishing companies both are heavily reliant on data in their operations; however, each defines its own critical data sources differently (O’Bannon, 2006). Examples of critical data resources include inventory records, personnel information, orders, invoices, payroll, customer databases, financial documents, mailing lists, and electronic data interchange forms from vendors and customers, social security numbers, credit card numbers (Ferelli, 2001; Hawkins et al., 2000; Janusz, 1993; Marlin, 2005; Marshall & Heffes, 2006).

Electronically stored data is not human-readable and instead is dependent on computer hardware and software to be meaningful. As Phillips (1999, p. 56) states, “without data, software is an empty shell”. While some data sources can be accessed by widely available hardware and software (e.g. word processing and spreadsheet documents on IBM-compatible PC’s), others are bound to specific software applications with custom install configurations. For example, if data is stored in a relational database format on quarter-inch magnetic tape, both hardware and software are needed in order to retrieve the data. Systems recovery is no small task and involves reinstalling and reconfiguring software, updating system drivers, and mapping data (O’Bannon, 2006). Disaster recovery methods, therefore, need to encompass both data and IS.

The consequences of losing critical data and IS can be financial loss, damage to reputation, or legal action (Gibb & Buchanan, 2006). Financial loss arises for many reasons including lost revenues, compensatory payments, future loss of revenue, loss of productivity and customer attrition (Freeman, 2000; LaPage & Gaylord, 2003; Lewis, 2005; Marshall & Heffes, 2006). Indirect financial impacts may be felt from damage inflicted on a brand or reputation (Eckert, 2006; Freeman, 2000). In financial industries, customer trust is of utmost importance and new legislation requires disclosure of customer data loss (Duke, 2006; Mearian, 2005). Businesses losing data invite exposure to litigation especially for data regulated by mandates such as HIPAA (Eckert, 2006; Freeman, 2000).

Managerial Planning

Following the identification and assessment of the risk of community-wide natural disasters affecting an organization’s critical data and IS is the managerial planning function. Consequently, devising both a comprehensive recovery plan and a plan to restore data were identified as two of the most important components of disaster recovery methods by small business executives. Regardless of what disaster recovery method is planned, the mode of governance can vary. Whereas certain methods are cost prohibitive to small businesses, they are often accomplished via the use third-parties. Hosting arrangements of data and IS by third-party service providers transfers risk and responsibility of disaster recovery away from the business. While this is ideal for the small business that lacks in experience or that opts to focus on core
Components of Disaster Recovery Methods, Cumbie

competencies, hosting sacrifices control of data deemed critical to sustained operations. If enacting a disaster recovery method is too complex and a hosting governance model is chosen, the small business must manage the relationship. Service level agreements outline the contractual obligation of a host provider and along with the host’s disaster recovery methods should be scrutinized to ensure they are up to par with expectations. Even when a hosted solution is chosen instead of an in-house solution, managers will need to have an understanding of disaster recovery methods in order to evaluate the choice of service providers. For example, both in-house solutions and chosen service providers need to have a media rotation strategy in place to avoid the loss or damage to any one storage media type.

Managerial Leadership

A disaster recovery plan, once chosen, needs to be communicated from managers to those who will conduct its operations. Managerial leadership is predicated the communication of the plan and also the manner in which communication occurs in an organization. Two disaster recovery components that relate to communication were identified among the most important by small business managers while two others were identified as also being important. These components include establishing a single communication touch-point, such as a toll-free telephone number, for employees to give and receive information during a disaster. Also, communication means alternative to the telephone were encouraged to maintain contact not only with employees but also with vendors and partners.

Managerial Organization

The managerial function of organizing includes the disaster recovery components related to an organization’s personnel. The literature review to reveal the necessary components of disaster recovery methods was conducted under the assumption that data and IS disaster recovery is important only so long as the personal safety of community members is ensured. For this reason, the presence of key personnel in the organization to enact a chosen disaster recovery method was overlooked. The results of the Delphi study reveal the mistake of overlooking the role of organization personnel. Among the most important components of a disaster recovery method that were identified by an expert panel of small business executives were ensuring technical IT expertise to perform the operations of a chosen method and to designate roles and responsibilities. Ensuring technical IT expertise to assess the value of data was also identified but not among the most important components.

Common Operational Components

To summarize thus far, specific disaster recovery methods depend on type of information security threat and type of data loss. The plethora of disaster recovery methods available to study is thus narrowed down to those pertaining to the
context of community-wide natural disasters and both transactional and historic data loss. Data and IS systems resources critical to a business must be identified so that a commensurate disaster recovery practice can be enacted. Following the managerial functions surrounding the decisions involved in selecting disaster recovery and consistent with Gibb & Buchanan’s (2006) business continuity framework, the next logical step is to enact the planned disaster recovery method. Prior to discussing the actual methods, four components common of an effective portfolio of components of disaster recovery methods are identified. Methods employed by small businesses in response to natural disasters must achieve regulatory compliance, digitization, centralization, encryption, and geographical diversity.

**Regulatory Compliance**

The degree to which an organization is subject to regulatory mandates such as Sarbanes-Oxley Act, SEC Rule 17a-4, and HIPAA will influence the adopted disaster recovery methods. In the presence of a mandate, certain procedures by which data is stored and transported are determined by a regulatory agency. Adherence to applicable mandates is a driving force of adopting disaster recovery in general, and what method is selected.

**Digitization**

The degree in which organizational data are in electronic or digital formats increases an organization’s ability to enact an effective disaster recovery method. Despite the numerous threats to digital IS, digitization is essentially a prerequisite to the adoption of any disaster recovery method by allowing data to be easily copied, transported, and stored when compared to paper-based documentation (Eckert, 2006).

**Centralization**

One component of disaster recovery methods identified as being among the most important by an expert panel of small business managers is to maintain all critical data centrally, e.g., on servers opposed to personal computers. Centralizing data does not preclude the existence of critical data on distributed IS or IT components but does entail that dispersed data and IS are periodically and routinely collected on a central system. From a central point, data and IS can be efficiently protected against disasters.

**Encryption**

At some point in the process of disaster recovery, data and IS will be transported off-site at the expense of security. Once data-at-rest becomes data-in-transit, the risk of human threats such as theft, damage, or loss significantly increases
Components of Disaster Recovery Methods, Cumbie

(Kontzer & Greenmeier, 2006). Encryption of the data minimizes the impact of a lost or stolen backup at the expense of increased complexity (Mearian, 2005). For each method discussed, encryption is a necessary component.

Geographical diversity

Disaster recovery methods are enacted either in-house or off-site. In-house methods are useful because data is on-hand instead of another location but are an inadequate defense against a natural disaster of the magnitude of Hurricane Katrina of 2005. An expert panel of small business managers identified the storage of digital media to be off-site and at a geographically diverse location as an effective disaster recovery component. In the case of a geographically far reaching natural disaster, community infrastructure is likely damaged and evacuation is mandated. The alternative site must be located beyond the geographical span of the identified risk. Remote access to data and IS were also identified among the most important components of disaster recovery methods by an expert panel of small business executives. Remote access counterbalances the geographical relocation of data and IS by providing continued access, for example, to e-mail via the Internet.

Variable Operational Components

Given the common components of method being compliant, digitized, encrypted, and geographically diverse, specific methods appropriate for small businesses identified from a review of practitioner-oriented literature are classified by 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). Practitioner-oriented literature explicitly identifies RTO as a critical determinant of what practice to use (Connor, 2006b; Ferelli, 2001; O’Bannon, 2006; Patrowicz, 1998). RTO is implicitly conveyed in discussions of data accessibility; immediately accessible data calls for an immediate RTO (Eckert, 2006). As a rule, the less time specified by an RTO, the more expensive the practice will be (Connor, 2006b). Therefore, the value of continual access to organizational data must be weighed against the cost of the recovery practice.

Near-Immediate Recovery Time Objective

The most demanding RTO requires an online data-oriented disaster recovery practice in conjunction with fully redundant IS, or a hot site. Verisign, Inc. is a leading provider of online digital certificates and requires continuous data access and an therefore an immediate RTO. Their adopted practice is a hot site, or an off-site computer-ready facility that can sustain business operations after a disaster (Essex, 2000; Patrowicz, 1998; Phelan & Hayes, 2003). With a hot site solution, data is synchronously mirrored in a redundant system which takes over if the original system fails. Transaction-intensive businesses, such as an online service provider like Verisign, require the most immediate RTO’s and therefore use off-
Components of Disaster Recovery Methods, Cumbie

Site redundant facilities, such as hot sites with electronic vaulting. This practice uses dedicated telecommunication lines transmit data synchronously to a redundant system that can seamlessly continue operations when the primary site fails (Connor, 2006a; Ferelli, 2001; Phelan & Hayes, 2003).

Whereas a hot site is a disaster recovery practice encompassing both IS and data, a cold site maintains computer-ready facilities that are capable of supporting operations but are not equipped with data or IS (Patrowicz, 1998). This option is less expensive than maintaining a fully redundant IS facility and likewise is suitable for a less immediate RTO. Quick shipping arrangements with vendors can provide delivery of IS hardware to cold sites within three to five days (Patrowicz, 1998; Phelan & Hayes, 2003). Upon receipt, installation and configuration of IS hardware, data can then be restored from online or external sources.

Delayed Recovery Time Objective

Immediate RTO’s are measured in seconds to minutes, thus requiring on-line disaster recovery practices. By contrast, less stringent RTO’s measured in hours or days rely on periodic backups and stored on high-capacity, but slow external media. These RTO’s utilize external media such as tape drives, floppy disks, external hard-drives, CD’s, DVD’s, removable media (LaPage & Gaylord, 2003; Moore, 1999; O’Bannon, 2006). External media have the most storage capacity per cost than any other backup medium. The lower cost comes at a price of accessibility speed, an attribute compatible with a delayed RTO. Several different options of external media are available, however just as diversity is important geographically, so is the importance of diversification of storage media. Tape-based or optical media options have a life expectancy of ten years or less for major brands and 50 years or less for high quality brands (Betts, 1999). In this vain, no single media should be relied upon for disaster recovery. A media rotation strategy calls for different media to be regularly rotated. Rotation reduces the risk of a single media type becoming damaged during storage. For that matter, media needs to be stored securely in an environment that protects from harmful agents such as heat and water.

The Grandfather/Father/Son media rotation practice provides the most resilience to media failure and data loss, using a variety of storage media and both full and incremental backups (Buffington, 1997; NPower). A full backup duplicates all data, a simple yet inefficient practice. Selective backups require the user to choose which data to backup and requires more thought and introduces the potential for important data to be overlooked. Incremental backups are conducted after a full backup and only duplicate the data that has changed since the last time a backup was conducted. The Son backup practice uses only a single media to conduct a full backup every day. Although easy and inexpensive, this practice is vulnerable to media failure from frequent handling and reuse and also is incapable of reverting back to data more than one day old. The Father/Son practice uses six media, conducting incremental backups Monday through Thursday and alternating media every other Friday to conduct a full backup that is stored off-site. The Grandfather practice uses nineteen media,
adding an additional full backup on the third Friday and twelve monthly full backups stored off-site. The culmination of these practices, Grandfather/Father/Son, provides balance of media use over a forty week period (NPower).

Testing Operational Components

A chosen disaster recovery methods that satisfies the common components and is determined by RTO is not yet complete until the overall disaster recovery method is tested to ensure the restoration of data and IS. This step is a vital but often overlooked component of disaster recovery (Gibb & Buchanan, 2006; Mearian, 2005). An expert panel of small business executives did not overlook this final step, identifying that a plan to restore the data is among the most important components; testing the restoration with alternative hardware and simulating an emergency were also identified but not as being the most important. A failed restoration at the critical moment after a disaster may be no different than if no disaster recovery methods were enacted. While this step may require extra planning, a survey revealed that 34% of businesses fail to test their plans and of those that do 77% experienced failures (Essex, 2000; Lewis, 2005).

Summary of Disaster Recovery Methods

The components are divided into two categories, managerial and operational, and are illustrated in Figure 2. The first category includes the controlling, planning, leading, and organizing functions that identify risks to critical organizational data and IS and then develops and communicates a plan and staffs and delegates organizational roles to enact the plan. Operational components include those common to any disaster recovery method: compliance, digitization, encryption, and geographical diversity. Compliance is a necessary but insufficient step toward protecting data and IS while digitization is fundamental to the use of computer-based IS and non-digitized organizational data, i.e. paper-based, are many times more difficult to duplicate, store, transport, and preserve. Encryption is based on the fact that organizational data at some point will be transported and stored at an alternative location. The numerous examples of lost or stolen data underscore the possibility of not retaining data which in turn exposes an organization to anything from a denigrated reputation, to a loss of customers and revenues, to litigation. Finally, geographical diversity must be achieved so that data and IS can exist beyond the geographical scope of a community-wide natural disaster.

Upon satisfying these common components, an organization’s RTO leads to which disaster recovery method will satisfy the minimum time an organization cannot operate without access to its data. An immediate or near-immediate RTO require a high-degree of redundancy: a hot site with fully redundant facilities, hardware, systems and software, and data synchronized with operational data; a cold site with an alternate location with computer-ready facilities used in conjunction with pre-arranged quick-ship of computer equipment from vendors. The redundancies necessary for a demanding RTO is cost-prohibitive to many organizations especially small businesses. These methods are usually accomplished through a third-
party service provider. In this case, the focus is shifted from managing disaster recovery methods to managing service providers to ensure contractual obligations are met, to identify stable service providers who will be in operation in the future, and to choose those providers with satisfactory customer service.

![Testing Diagram]

Figure 1. Essential Components of Disaster Recovery Methods

For organizations with a less demanding RTO, the disaster recovery method of data backup will suffice. Again, organizations may resort to the use of a third-party service provider to host backed up data locally or over a network and the same issues of governance will apply, i.e., evaluating a service provider’s adherence to the essential components of a disaster recovery method. Once stored on media, data then needs to be stored off-site in a secure and environmentally controlled facility.

Regardless of RTO the final component of an effective disaster recovery method is testing to provide assurance of successfully restoring organizational data and IS and resuming business operations. The absence of testing is essentially equivalent to not preparing and is even worse because of the resources that were allocated to disaster recovery are precluded from use in other business functions. Based upon the results of the testing and restoration, an evaluation of the efficacy of the disaster recovery is made that informs the managerial control function and begins the entire disaster recovery method decision process anew.
Discussion & Conclusion

The comprehensive portrait of essential components of disaster recovery method that relate to a reduced likelihood that a community-wide natural disaster will result in unrecoverable losses of electronically stored organizational data and IS was developed by examining practitioner-oriented literature and conducting a Delphi study. Of the three goals of research methods: generalizable results, precise measures, and a realistic context, the Delphi method achieves realism at the expense of the two other goals (Scandura & Williams, 2000). As evidenced by the scarcity of academic research (Kotulic & Clark, 2004), this research topic is considered to be developmental and therefore merits qualitative studies to address a research problem from a local perspective rather than from that of researchers (Rogers, 2003). This serves to maximize realistic contexts and eliminate researcher-bias so that subsequent research can develop precise and generalizable measures.

The resultant portrait of disaster recovery methods consists of managerial and operation components. Ultimately, the true test of these components is, when enacted, the resilience of organizational data and IS after a community-wide natural disaster. This portrait is presented so that the extent of adoption of disaster recovery can be measured among small businesses. Measuring the extent of adoption is a precursor to invoking theories such as innovation diffusion that offers cognitive and social antecedents to an adoption decision. Encouraging the adoption of disaster recovery among vulnerable but economically-critical small businesses is vital to protect storm-embattled communities. The disaster recovery portrait resulting from this study is a step toward encouraging organizational and community vitality.

References


Components of Disaster Recovery Methods, Cumbie


The full review was removed due to length constraints and is available from the author upon request.

2 The list of ten articles was removed due to length constraints and is available from the author upon request.