Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

DEVELOPING THE IT DISASTER RECOVERY PLANNING CONSTRUCT

JORDAN SHROPSHIRE
INFORMATION TECHNOLOGY DEPARTMENT
GEORGIA SOUTHERN UNIVERSITY
jshropshire@georgiasouthern.edu

CHRISTOPHER KADLEC
INFORMATION TECHNOLOGY DEPARTMENT
GEORGIA SOUTHERN UNIVERSITY
ckadlec@georgiasouthern.edu

ABSTRACT

IT disaster recovery planning is no longer an option. Reliable IT services have become an integral part of most business processes. To ensure the continued provision of information technology, firms must engage in IT disaster recovery planning. Surprisingly, there is little research on this topic. The authors posit that this is because IT disaster recovery planning has not been fully conceptualized in mainstream IT research. Thus, this article describes a three part study in which the creation of a domain definition precedes the development and evaluation of an empirically reliable and valid measure of IT disaster recovery planning. A previously-validated framework was followed in order to create the 7 dimension, 34 item measure for assessing the degree of IT disaster recovery planning. The measure was validated using a sample of 153 banking and finance firms. Practitioners can use the results of this study to guide IT disaster recovery planning; academics may use the measure to compare planning activities among firms.

Keywords: disaster recovery planning, measures, information technology, construct development

INTRODUCTION

In August 28, 2005, some 63 major enterprises were headquartered in Louisiana. By the end of October, over 15% of these firms ceased to exist [45]. In their final communications with investors, many of these firms indicated that the loss of critical IT services was a crippling blow to their survival [92, 99]. This event should have set a precedent for the current generation of IT managers, but many firms still have a lax attitude toward IT disaster recovery planning [27]. For instance, in a recent study it was found that 28% of IT executives either do not know what their plan to continue is or know they do not have one [5]. For those organizations that have full scale data centers, 22% respond that their plan needs work [93]. Unless this situation is addressed, many more organizations will inevitably fail to recover from IT-related disasters.

While Information Technology Disaster Recovery Planning (ITDRP) is occasionally addressed in IS/IT textbooks [28] and is generally regarded as an important managerial activity [38, 53, 81], it is rarely approached in mainstream research. (Only 6 articles on IT disaster recovery planning were published in peer-reviewed MIS journals in the past ten years.) ITDRP blends technical, behavioral, managerial, and sociological perspectives - core competencies for IT/IS researchers [98]. These conditions culminate in a rare opportunity to pursue research which can be rigorous and immediately relevant. However, ITDRP will require additional clarity and direction before it will be studied in a more meaningful way. Thus, this is a foundational study, laying the groundwork for future research. This project contributes an important first step by providing a domain definition of ITDRP which is grounded in practitioner-oriented literature and provides a 34 item measure for assessing the degree to which organizations engage in IT disaster recovery planning.

This study is organized into three parts following the background section. In the first part, the domain definition is derived. In the second part, the development and validation of the construct's measure is reviewed. The third part describes the empirical evaluation of the measure's properties. Following this, implications for practice and research are presented. Finally, concluding comments are given.

BACKGROUND

It appears that IT disaster recovery planning practices tend to lag behind contemporary trends in information technology. Even though modern enterprises have sophisticated information systems upon which they are utterly reliant, their IT disaster recovery plans may be limited to backing up data and devising methods for restoring data resources [47, 79]. Considering the integration of IT into all business functions and the reliance on technology, this view of ITDRP has become outdated [42]. Furthermore, rapid changes in business processes and organization structure necessitate a clarification of five points concerning IT disaster recovery planning:

First, although the terms "IT disaster recovery planning" and "business continuity planning" are occasionally used interchangeably, they are separate processes [40]. Business continuity plans are holistic strategies for keeping businesses operational following disaster [1, 19]. IT disaster recovery plans are aimed specifically at restarting IT services. In this role, they support business continuity plans [16]. The aims and objectives of IT disaster recovery plans should not conflict with those of business continuity plans.

The second point concerns the classification of incidents as IT disasters. IT disasters impact the organization in which the IT service is employed; including IT services which are outsourced to an independent vendor [20, 58]. If the vendor somehow fails to provide an IT service, its clients may be faced with IT disaster [41]. IT disasters range from the accidental deletion of a file to a hurricane which destroys the building that houses the data center [84]. IT disasters may also stem from damage to supporting infrastructure in the area of the data center. These events cause damage to the inputs which collectively provide IT service. When the damage is such that it is no longer possible to provide an IT service, then an IT disaster is said to have occurred [34, 61].

Third, it should be noted that IT disaster recovery is for restoring IT services, but not necessarily restoring specific hardware and software architectures [83, 39, 66]. Examples of IT services include internet connectivity, telecommunications, and data storage and processing. IT services add value by providing additional capabilities to organizational members. The provision of such services relies on a combination of inputs from multiple resources, including hardware, software, data, human resources, and utilities [56]. Because these inputs may be destroyed in a disaster, it may not be possible or practical to return to pre-disaster conditions. Thus, disaster recovery for an IT service is complete when the service has been brought back online in a stable condition [83, 39].

Fourth, ITDRP does not involve the simplification or discontinuance of IT services [65, 30]. The purpose of ITDRP is not to simplify IT services so that they are easier to restore. Nor does it involve risk mitigation. While these are important functions, they are not part of ITDRP. Instead, the focus should be on devising alternatives means of restoring services following disaster [38].

Finally, since there are many interrelated IT services in an organization and there is a limited amount of resources to support these services, any action performed should be considered as continuous as opposed to discrete. Backups have long been viewed as a necessary part of ITDRP but backups are not discrete in that it is not an all or nothing condition. Backups can cover many parts of the systems but not all or they can be incremental and not cover instantaneous changes.

CONCEPTUAL DEVELOPMENT

The first phase of the study focuses on creating a domain definition which is grounded in IT practitioner-oriented literature and developing a comprehensive list of the dimensions which represent the construct. This process follows a highly rigorous methodology [58] which has been repeatedly been used for construct development [50, 60, 96, 101].

Method

The definition of the ITDRP construct was derived using content analysis. Content analysis is a research method used in the social sciences to draw inferences from text [102]. In this case, the text includes articles which concern IT disaster recovery planning. Each reference to an aspect of IT disaster recovery was categorized according to an a-priori coding scheme. The results of the coding operation were iteratively refined into clusters which formed the basis of the construct dimensions and conceptual definition. This qualitative methodology is often used by information systems researchers to define concepts and frameworks in cases in which little research currently exists [14, 58, 94].

Sample

The population consists of all periodical articles which discuss IT disaster recovery planning. The sample was drawn from this population as follows: the Pro-Quest Direct and Business Source Complete databases were queried using keywords such as "IT," "disaster recovery," and "plan." Keywords were combined using Boolean search terms in order to achieve more specific results sets. Some 121 articles were initially found. After an initial inspection, 39 were culled because the content in the articles was not in any way related to this study. For example, several articles used the keywords "disaster recovery," but were focused solely on humanitarian issues following natural disasters; other culled articles discussed the civil engineering aspects which follow major disasters. An additional 10 articles did not contain any useable recommendations. Thus, 72 articles were ultimately included in the sample (see Appendix A). It should be noted that the majority of the articles were published in trade publications, industry-specific magazines, and IT practitioner–oriented journals; only 6 manuscripts came from academic or peer-reviewed sources. Many were written for audiences in the health care and financial fields.

Recording Units

Specific references to IT disaster recovery planning were identified in the articles. Each individual reference is referred to as a recording unit. For this research, each recording unit is defined as an idea regarding what should be included in the process of IT disaster recovery planning. Each specific IT disaster recovery planning recommendation was treated as a different recording unit to code. Thus, a sentence which reads "organizations should create backup copies of data and store backups offsite" would be coded in two separate units, with each idea belonging to only one category [52].

Coding Scheme

An a priori coding scheme was used to categorize the data [89]. The coding scheme was initially based on a list of 9 elements of an IT disaster recovery plan [28] (see Appendix B). This list is unique in that it does not advocate specific treatments, but provides general recommendations to consider when crafting an IT disaster recovery plan. This list was used to categorize the recording units derived from the first ten articles. After independently coding the first ten articles, the authors compared amendments and extensions to the coding scheme. Problematic portions of the coding scheme were addressed; categories were modified to the extent that they became mutually exclusive and exhaustive. As a result, the list eventually grew to a scheme of 30 elements (see Appendix B). This method has been advocated by qualitative researchers such as Weber [102]. Although the process of encoding is inherently subjective, it is expected that this can be minimized by taking additional steps such as coding independently and comparing results. The amended scheme was applied to the remainder of the units. Periodic quality control checks confirmed the enumeration.

Clustering

A total of 572 recording units were identified and coded. The resulting data were organized into a series of 7 IT disaster recovery planning dimensions and 16 subdimensions. As with coding, clustering is a qualitative research technique. Thus, the most rigorous method of clustering was used [52]. The technique by which the clusters were created follows a series of 3 steps: First, the units which were most similar were identified. By similar, it is meant that their merger would have the smallest effect on the observed differences in the data as a whole. Second, the units were grouped together, taking account of the losses incurred within the newly-formed cluster. Third, the data were modified to reflect the latest configuration of clusters on which the next merger is computed. This procedure was repeated until nothing more could be merged without changing the meaning of the data.

Results

The results of the content analysis and subsequent clustering led to the development of a conceptual definition of IT disaster recovery planning: the set of actions (IT disaster identification and notification, preparing organizational members, IT services analysis, recovery process, backup procedures, offsite storage, and maintenance) which an organization follows in order to improve its ability to resume IT services following a disaster (see Table 1). Although the articles in the content analysis prescribed specific recommendations or unique IT disaster recovery plans, the construct is defined in relatively global terms. Additionally, each of the recommendations would have to be applied to all IT services to the fullest extent to be considered complete. Compliance is then a continuum and not discrete. Because the definition is independent of specific technologies, IT architectures, and organizational governance schemes, it can be applied to a wide range of organizations. The following sections describe the dimensions of the definition.

Table 1: Dimensions of the IT Disaster Recovery Planning Construct

Dimension	Description	Sub-Dimension	Description
IT Disaster Identification and Notification	Procedures which have been developed for detecting IT disasters, for communicating during emergencies, and for warning IT disaster recovery team members and other stakeholders.	Detection	Procedures for detecting IT disasters.
		Warning	Procedures for informing IT disaster recovery team members and stakeholders that an IT disaster has occurred.
		Means of Warning / Communication	Establishment or formalization of communication channels to be used in the event of an emergency.
Preparing Organizational Members	Procedures for IT disaster recovery team training, briefing for key non-team members, and the formalization of a decision-making structure.	ITDR Team Preparations	Team assignments and responsibilities during the disaster.
		Non-ITDR Team Preparations	Training and briefing of non-team members in the event of a disaster.
		Decision Making	Formalization of a decision making structure.
IT Services Analysis	Procedures for cataloging IT services, prioritizing IT services in terms of reactivation, and identifying potential threats.	IT Services Identification	Identification of IT services.
		Prioritizing IT Services	Listing of the order in which services need to be reactivated.
		Risks to IT Services	Identification of risks to IT services and infrastructure.
Recovery Process	Procedures for restoring IT service inputs and for switching IT operations to alternative facilities.	Recovery Procedures	Alternative facilities and procedures for switching operations to those facilities.
		Alternative Facilities	Recovery procedures for service inputs such as human resources, facilities, communications technologies, servers, application systems, and data.
Backup Procedures	The degree to which a routine has been developed for creating backups.	Backup copies of data, software, configuration files, and IT disaster recovery plans.	
Offsite Storage	Procedures for ensuring that systems, software and data are made as portable as possible, and those offsite locations have been selected for use as backup storage sites.	Portability	Procedures for ensuring that systems, software, and data are as portable as possible.
		Offsite Backup Locations	Offsite locations to backup data, software, configuration files, the IT disaster recovery plans.
Maintenance	Procedures for testing and updating the IT disaster recovery plan and its associated documentation and for ensuring that the IT disaster recovery plan fits within the scope of the business continuity plan.	Testing and Updating	Procedures to ensure adequate testing and updating of the disaster recovery plan.
		Documentation	Documentation of configuration and changes to systems, hardware, and software.
		Synchronizing	Procedures to ensure the IT disaster recovery plan is part of the business continuity plan.

IT Disaster Identification and Notification

The first dimension, *IT disaster identification and notification*, is based on the procedures which have been developed for detecting IT disasters, for communicating during emergencies, and for warning IT disaster recovery team members and other stakeholders. This dimension of the IT disaster recovery planning construct is comprised of three sub-dimensions: *detection*, *warning*, and *means of warning / communicating*. The detection sub-domain is based on the identification of IT disasters. This includes procedures for distinguishing between a loss of service inputs and a loss of IT services. The warning sub-domain includes actions which are taken to warn IT disaster recovery team members (those individuals responsible for restoring IT services) that a crisis has occurred. This alarm serves as a catalyst to jumpstart the recovery process. Procedures for alerting key stakeholders (such as senior managers, directors, and members of a business continuity planning team) should be included in the second sub-dimension. The final sub-dimension, means of warning/communication, represents the establishment or formalization of communication channels to be used during the disaster. During emergencies, wireline phone systems may be down or employees may be forced to evacuate geographic location. In such cases, it is still necessary to contact them. Alternative channels might include web-based message centers, calling trees, or exchange of mobile phone numbers.

Preparing Organizational Members

This dimension of the IT disaster recovery planning construct includes procedures for IT disaster recovery team training, briefing for key non-team members, and the formalization of a decision-making structure. Preparing organizational members is based on three sub-dimensions: *IT disaster recovery team preparations*, *non-IT disaster recovery team preparations*, and *decision making*. The first sub-dimension concerns the organization IT disaster recovery team. This team consists of those individuals who are necessary to recover IT service inputs. The team may include individuals outside the IT department. For example, cable/electrical repair technicians or facilities workers may also be considered part of the IT disaster recovery team. Procedures for acquainting team members with their responsibilities and providing training are included in this sub-domain. The second sub-dimension addresses the training and briefing of non-team members in the event of a disaster. Key stakeholders must appreciate the implications of IT disasters, and understand what do when IT services are down; thus they must also receive some degree of training. The final sub-dimension, decision making, addresses procedures for decision making authority under a variety of circumstances, such as when key employees are missing, incapacitated, or otherwise unable to exercise their decision making authority.

IT Services Analysis

IT service analysis includes three sub-domains for cataloging IT services, prioritizing IT services in terms of reactivation, and identifying potential threats. The first sub-domain, *IT services identification*, involves the exhaustive review of all the services which an IT department offers to other departments within an organization. As with many other components of the IT disaster recovery planning construct, this sub-domain focuses on IT services, such as email communication, not on IT service inputs, such as Exchange servers, routers, or client applications. The second sub-domain, *prioritizing services*, involves procedures for ranking IT services in the order in which they should be restored. This involves identifying dependencies of the services and the relative importance of each service to the business's continuity. The third sub-domain focuses on the identification of risks to IT services and associated infrastructures. Again, the focus is on the IT service, not the service inputs. This is because it may be possible to continue offering an IT service even if a particular service input is down. For example, two of three servers may be offline, but a third server may support the continued functioning of an IT service.

Recovery Process

This dimension of the IT disaster recovery planning construct includes procedures for restoring IT service inputs and for switching IT operations to alternative facilities. It is made up of two sub-dimensions: *recovery procedures* and *alternative facilities*. The first sub-dimension focuses on the process of restoring basic IT service inputs. Although specific service inputs were found to differ widely among organizations, the results of the cluster analysis yielded six general categories: human resources, facilities, communications technologies, servers, application systems, and data. The human resource category involves the individuals who perform the labor needed to deliver IT services. The facilities category involves restoring IT service inputs of a physical nature, including building structures, utilities, and heating/cooling. The communications category includes inputs needed to convey video, voice and data. Elements of this category may range from PDAs and smartphones to the cabling needed to connect local area networks. The server category includes physical hardware for managing network resources. The application systems category is a mixture of hardware and software supporting end users' computing needs. This categorization exposes how much planning must take place to bring IT services back online following disaster, and shows how inseparable the human elements is from the service. The final category of service input is data; raw, unprocessed facts and figures. The other sub-dimension involves the procurement of alternative facilities for hosting IT operations in the event that a primary site goes offline; it also includes plans for the orderly migration of operations to the alternative site in emergencies.

Backup Procedures

This dimension of the IT disaster recovery planning construct is based on routines developed for creating backup copies of data, software, configuration files, and the IT disaster recovery plan. Unlike other parts of the IT disaster recovery planning construct, this component is unidimensional.

Offsite Storage

Offsite storage includes procedures for ensuring that systems, software and data are made as portable as possible, and that offsite locations have been selected for use as backup storage sites. This dimension of the IT disaster recovery planning construct is comprised of two sub-dimensions: *portability* and *offsite storage*. The portability component represents a firm's efforts at organizing data, software, and other documents into formats which are as easy to transport as possible. The second component, off-site storage, concerns procedures for transporting and storing data, software, configuration files, and copies of the IT disaster recovery plan at alternative locations.

Maintenance

The *maintenance* dimension is based on plans for testing and updating the IT disaster recovery plan and its associated documentation, and for ensuring that the IT disaster recovery plan fits within the scope of the business continuity plan. Maintenance is based on three sub-dimensions: *testing and updating*, *documentation*, and *synchronizing*. The first sub-dimension, testing and updating, includes procedures for continually testing and updating an IT disaster recovery plan. Tests are conducted to ensure that the IT disaster recovery plan will work in the event of an IT disaster. The plan is updated to account for changes in IT services and service inputs, and to correct shortcomings identified in the course of testing. The second sub-dimension concerns a related issue: updating documentation such as configuration manuals, network schematics, and change logs on a regular basis. Such documentation might not be incorporated into an IT disaster recovery plan, but might be useful in the event of an emergency. It is not possible to predict every threat to IT services and service inputs, thus the recovery process should not be considered completely comprehensive. In cases where it is necessary to devise new plans or modify existing plans for restoring service inputs, such documentation will prove useful. The final sub-dimension, synchronization, ensures that the IT disaster recovery plan falls in line with the business continuity plan.

Summary

This part of the study represents one of the first efforts at providing a systematically-developed definition of IT disaster recovery planning. The dimensions, *IT disaster identification and notification*, *preparing organizational members*, *IT services analysis*, *recovery process*, *backup procedures*, *offsite storage*, and *maintenance*, collectively comprise the actions which firms must take in order to ensure recovery from It disasters.

MEASURE DEVELOPMENT

This phase of the study focuses on developing a measure for ITDRP based on the domain definition created in the previous section. Along with the domain definition, a list of specific activities associated with ITDRP was developed. The items from this list were used to generate the statements for the first version of the measure (see Appendix C). This section describes the process by which content validity was assessed and the measure was iteratively refined.

Method

The emphasis of this stage is survey pretesting and item screening. The pretest is the first attempt to get empirical feedback from a controlled sample to assess the appropriateness of the instrument. The results of the pretest were taken into consideration and the survey was revised. Next, item screening was conducted using the procedure described by Lawshe [57]. Essentially, this is a quantitative approach to conducting content validity analysis. The results of this exercise were used to further refine the measure.

Pretest

The original survey contained 53 scale items; each item represented a separate aspect of ITDRP. The items were used to characterize the respondent's perceptions of IT disaster recovery planning in their organization. Because organizations can't perceive phenomena and respond to surveys, individuals are surveyed as their proxy [63]. Thus, the survey was designed to capture IT professional's judgments regarding the degree of IT disaster recovery planning activities in the organization. Scale responses were gauged using 5-point Likert scales, in which 1 represented "strongly disagree" and 5 represented "strongly agree."

Pre-testing was conducted using a carefully selected panel of subjects who were knowledgeable about IT disaster recovery planning. Three categories of respondents were asked to participate, including IT faculty, IT practitioners, and instrumentation experts. A total of 6 individuals were selected, two for each category. Each was given a paper copy of the questionnaire and a self-evaluation form. Respondents were asked to complete the survey instrument first and then critique the survey regarding format, content, understandability, readability, and ease of completion. In addition, respondents were asked to identify items that should be included in the survey or left out. All responses were considered and modifications to the survey were made based on the feedback. As a result, the survey was refined to consist of 42 items.

Item Screening

A quantitative procedure was used to empirically assess the content validity of the survey [57]. This method determines whether each item on the survey adequately represents the content domain of the construct. This approach to content validity employs a panel of individuals with experience in IT management and disaster recovery planning. Some 9 IT professionals were given a copy of the revised instrument and asked to rate the degree to which each item was relevant to ITDRP. Each item was rated using a three point scale, in which 1 corresponded with "not relevant," 2 corresponded with "important (but not essential)," and 3 corresponded with "essential."

From the gathered data, a content validity ratio was calculated for each item (see Table 2). Although Lawshe only used the "essential" response category in calculating the CVR, a less stringent criterion was justified since "important" and "essential" are both positive responses. The CVR for each item was evaluated using the statistical inference table published by Lawshe [57]. Items with statistical significance are interpreted to possess some level of content validity; these items were retained. Those which are not statistically significant were dropped. As a result, 34 survey items remained; these form the basis of the final version of the survey (see Table 2).

Table 2: Content Validity Assessment of Item

Item		*AVE*	*CVR*
I1	We have procedures for detecting IT disasters	3.89	.77
I2	We have a means of assessing the magnitude of IT disasters	3.77	.81
I3	We have procedures for alerting individuals responsible for IT disaster recovery	3.78	.86
I4	We have procedures for letting stakeholders know that an IT disaster has occurred	3.95	.76
I5	We have established an alternative means of communications (i.e. cell phones) to use in emergencies	3.70	.75
P1	We have an IT disaster recovery team (i.e. a group of employees who are responsible for restoring IT)	3.91	.66
P2	Those responsible for IT disaster recovery have been assigned specific tasks for restoring IT services	4.00	.79
P3	Employees and other stakeholders know what to expect during IT disasters	3.87	.85
P4	We have an explicit chain of command for dealing with IT disasters	3.60	.71
S1	We have identified all IT services which the IT department offers	3.85	.76
S2	We have identified all system resources required to provide IT services	3.88	.82
S3	We have assessed risks to IT services and infrastructure	3.94	.75
S4	We have ranked the order in which IT services would be repaired, if a disaster occurred	3.91	.69
R1	Should our primary site go offline, we have a secondary site	3.80	.77
R2	Should our primary site go offline, we have procedures for relocating IT operations	3.97	.81
R3	Our plans account for possible losses of human resources (i.e. missing or injured IT workers)	3.89	.75
R4	We have procedures for restoring physical facilities such as physical buildings, power, and cooling systems	3.51	.66
R5	We have procedures for recovering communications technologies such cellular phones, email, and VOIP	3.70	.54
R6	We have procedures for recovering servers	3.91	.71
R7	We have procedures for recovering applications and software	4.03	.82
R8	We have procedures for recovering data	4.04	.89
B1	We have procedures for creating backup copies of data	4.15	.91
B2	We have procedures for creating backup copies of software	4.08	.66
B3	We have procedures for creating backup copies of configuration files, change logs, and other documents	3.89	.84
B4	We have procedures for creating backup copies of the disaster recovery plan itself	3.80	.71
O1	We have ensured that system resources are as portable as possible (i.e. that they can be transported)	3.46	.78
O2	We have offsite locations for storing data	3.70	.64
O3	We have offsite locations for storing software	3.99	.81
O4	We have offsite locations for storing configuration files, change logs, and other relevant documents	3.68	.75
O5	We have offsite locations for storing copies of the IT disaster recovery plan	3.64	.78
M1	We have procedures for testing of the IT disaster recovery plan	3.89	.81
M2	We have procedures for updating the IT disaster recovery plan	3.90	.76
M3	We have procedures for ensuring that the IT disaster recovery plan is part of the business continuity plan	3.88	.74
M4	We have procedures for documenting system configurations, changes, and updates	3.98	.81

The dimensions and sub-dimensions and the final 34 items are represented in Table 3.

Table 3: Dimensions of the IT Disaster Recovery Planning Construct and associated Measures

Dimension	Sub-dimension	Item
IT Disaster Identification & Notification Procedures	Detection	I1
		I2
	Warning	I3
		I4
	Means of Warning	I5
Preparing Organizational Members	ITDR Team Prep.	P1
		P2
	Non-Team Prep.	P3
	Decision Making	P4
IT Services Analysis	IT Services	S1
		S2
	Risks to Services	S3
	Prioritizing IT Services	S4
Recovery Process	Alternative Facilities	R1
		R2
	Recovery Procedures	R3
		R4
		R5
		R6
		R7
		R8
Backup Procedures		B1
		B2
		B3
		B4
Offsite Storage	Portability	O1
	Offsite Locations to Backup	O2
		O3
		O4
		O5
Maintenance	Testing and Updating	M1
		M2
	Synchronizing	M3
	Documentation	M4

MEASURE EVALUATION

This phase of the study involves administration of the ITDRP measure and analysis of the resulting data. The sample consists of banks and financial service institutions. Because ITDRP was operationalized in terms of a formative measure, the scale items were analyzed according to widely-accepted formative development standards [72]. The results of the analysis support the measure.

Method

A survey was mailed to the chief executive officer of each firm. The directions in the cover letter requested that the survey be sent to the organization's IT director or to the individual responsible for managing the firm's information technology. Self-addressed stamped envelopes were included for returning completed surveys. As an alternative to mailing in a paper survey, the directions indicated that the survey could be completed online.

The address of a website containing the survey was provided. To ensure that each organization completed only one web survey, an authentication code was also included; after the code was used once, it could not be used again. Both the online and paper survey used the same instructions (see Appendix D) and participants rated their degree to which they agreed to the items in table 2 as Strongly agree, Agree, Neutral, Disagree, Strongly disagree.

Sample

For this research, the sample was comprised of member organizations of the Georgia Bankers Association (GBA). The GBA is over 120 years old; almost every bank in the state of Georgia is a member. To qualify for membership, an organization must be a state or federally charted bank. In total, the association is comprised of 337 member organizations. In terms of relevance, this population is somewhat unique in that banks are required to meet minimum IT disaster recovery planning standards set by the Federal Financial Institutions Examination Council (FFIEC) and the Federal Deposit Insurance Corporation (FDIC). This sample was intentionally selected because the respondents would have an understanding of the concept of ITDR planning due to these regulations.

Analysis

After purging incomplete surveys, there were a total of 153 useable records. This equates to a 45.4% response rate. Because the data were collected using various media, Wilk's Lambda and independent sample t-tests were conducted to ensure homogeneity; no significant differences were found.

Prior to further analysis, steps were taken to classify the constructs as formative or reflective. In contrast to reflective measures, where variation in the items reflects the construct's meaning, items in a formative scale are dimensions which together form the construct. Thus, changes in formative measures affect the meaning of the construct itself [25, 48, 72]. According to the decision rules outlined by Petter [72], the IT disaster recovery planning construct should be classified as formative. Thus, validity and reliability assessment followed the procedures specified for formative measures.

For formative construct analysis, content validity is established prior to data collection. Construct validity was assessed by considering the results of a principal components analysis (PCA) and examining item weightings [15]. Items were assumed to be valid if their weightings were significant [25]. The results indicated that nearly all of the item weights were significant at the .05 level of confidence (see Table 4). Some 6 indicators were slightly above the level of .05. However, these items were below the .06 level of confidence. Because of their importance in fully operationalizing ITDRP, the items were retained.

Because formative indicators need not co-vary, conventional tests of reliability are unjustified [64]. In fact, a high degree of reliability may even be undesirable. Indeed, it is suggested that if measures are highly correlated, it may suggest that multiple indicators are tapping into the same aspect of the construct [72, 25]. The VIF (variance inflation factor) statistic was used to ensure that items are not overly correlated [72, 25]. In this use, the recommended maximum threshold for the VIF statistic is less than or equal to 3.3 [15]. The calculated VIF statistics were all within the recommended range (see Table 4).

Table 4: Analysis of ITDRP Items

Dimension	*Item*	*Weight*	*t-Value*	*Significance*	*VIF*
IT Disaster Identification and Notification Procedures	I1	.177	1.791	ρ=.0507	2.132
	I2	.173	2.527	ρ=.0125	2.536
	I3	.189	2.100	P=.0374	2.436
	I4	.053	2.150	P=.0331	3.003
	I5	.017	2.868	P=.0047	2.800
Preparing Organizational Members	P1	.417	3.150	P=.0020	2.204
	P2	.173	2.942	P=.0038	2.030
	P3	.091	2.090	P=.0393	3.010
	P4	.201	2.478	ρ=.0143	2.236
IT Services Analysis	S1	.449	2.674	ρ=.0083	2.287
	S2	.243	2.343	ρ=.0204	2.868
	S3	.066	2.735	ρ=.0070	2.506
	S4	.155	2.082	ρ=.0390	2.326
Recovery Process	R1	.175	2.161	ρ=.0323	3.432
	R2	.086	2.109	ρ=.0366	2.707
	R3	.051	1.934	ρ=.0550	3.902
	R4	.006	1.951	ρ=.0529	2.010
	R5	.044	2.603	ρ=.0102	2.802
	R6	.264	2.665	ρ=.0085	1.985
	R7	.323	2.760	ρ=.0065	2.134
	R8	.135	2.675	ρ=.0083	2.822
Backup Procedures	B1	.248	2.047	ρ=.0424	2.064
	B2	.279	1.896	ρ=.0509	3.080
	B3	.344	1.947	ρ=.0534	2.123
	B4	.101	2.016	ρ=.0456	3.070
Offsite Storage	O1	.159	2.110	ρ=.0365	2.027
	O2	.310	2.551	ρ=.0117	1.111
	O3	.085	2.397	ρ=.0177	2.306
	O4	.107	1.973	ρ=.0503	2.700
	O5	.093	2.620	ρ=.0097	2.502
Maintenance	M1	.160	2.378	ρ=.0186	1.925
	M2	.537	2.981	ρ=.0033	3.083
	M3	.316	1.969	ρ=.0508	2.100
	M4	.066	2.527	ρ=.0125	1.904

Summary

As indicated by these tests, the items and the measure were found to possess suitable psychometric properties. In particular, sufficient variance was found in each of the items to ensure that they measure a continuum of responses. Removal or modification scale items were not warranted. Therefore, based on the evidence derived from this phase of the study, it is concluded that the measure is sufficiently valid.

IMPLICATIONS FOR PRACTICE

The intention of this article is to motivate IT managers to take action. Admittedly, the process may seem daunting, especially if the organization has not previously conducted any IT disaster recovery planning. Instead of jumping straight into planning activities, it is best to begin by developing a list of realistic planning goals for the next month, six months, and year. Depending on the complexity of information services, initial development of an exhaustive IT disaster recovery plan may take months of work. Initial training and disaster recovery team building is also time-intensive. These are examples of goals to set for the one year time-horizon. More immediate benchmarks should include the selection of an IT disaster recovery planning committee and an analysis of IT services. For the intermediate range, activities such as the identification of service inputs and elicitation of recovery procedures should be considered. Managing expectations by setting realistic targets is an important part of leading the ITDRP effort.

IMPLICATIONS FOR RESEARCH

IT disaster recovery planning, as a topic, is underserved. This article does not explore, in detail, any particular phenomenon. Rather, it attempts to provide a basis for further development. In an effort to build the knowledge base, IT/IS researchers should attempt to explore ITDRP from social, behavioral, technological, and managerial perspectives. Using the construct and measure developed in this paper, a number of intriguing questions may be asked. For example:

- How does ITDRP impact the IT disaster recovery process?
- What are the characteristics of organizations with superior ITDRP?
- How does organizational structure and IT governance relate to ITDRP?
- What is the relationship between organizational leadership and extent of ITDRP?
- Is there a link between ITDRP and corporate agility?

As the collective understanding of ITDRP grows, it is expected that researcher will ask more profound questions. As this information is developed and transferred to the next generation of IT managers, organizations will undoubtedly place more emphasis on ITDRP.

LIMITATIONS

One of the chief limitations of this study stems from the relative youth of ITDRP research. Highly-publicized disasters tend to build short-term interest in ITDRP, but after the story fades there is relatively little theoretical development. This research is among the first attempts to systematically define and measure IT disaster recovery planning. As such, it is possible that this definition will require further refinement in order to fully account for all its dimensions and sub-dimensions. Because the ITDRP measure was formative, it was not possible to conduct certain empirical analyses. The measure was subjected to comparable qualitative assessments. Although it is possible that such efforts can be subjective, every effort was made to perform as rigorous an analysis as possible. A final note concerns the sample population. It is recognized that banks are somewhat atypical with regard to IT disaster recovery planning. Unlike firms in other industries, they are required to meet minimum regulatory standards. Despite this, there was still considerable variance among banks. It is therefore suggested that this measure may be used by organizations in other regulated industries, such as healthcare, public service, and defense contracting.

CONCLUSION

This research delivers three important contributions. First, it draws attentions to the serious under-representation of IT disaster recovery planning research in the IT field. Second, it provides a basis for conducting work in this area by framing the concept of IT disaster recover planning and conceptualizing a definition grounded in practitioner literature. Finally, it provides a rigorously developed measure of ITDRP; this measure was empirically tested using a relevant sample population. Collectively, these efforts provide an initial first step toward a better understanding of the complexities of IT disaster recovery planning.

REFERENCES

[1] Anderson, J. “New trends in backup: Is your disaster recovery plan keeping up?” *The eSecurity Advisor*, 8, 2, 2008, pp. 58.

[2] Anthes, G. “Apocalypse Soon,” *Computer World,* Volume 42, Number 23, 2008, pp. 24-28.

[3] April, C. and Gryco, E. “Users fortifying enterprise walls,” *InfoWorld*, Volume 6, Number 10, 2001, pp. 17-20.

[4] Ashton, H. “How prepared is your business for a calamity?” *Japan Inc*, Volume 12, Number 1, 2008, pp. 15-17.

[5] AT&T “Business continuity survey: 2008,” *AT&T Reports*, Dallas, 2008.

[6] Baker, S. “Lessons learned: A devastating hurricane caused this CIO to rethink his carrier’s disaster recovery plans,” *Tech Decisions*, Volume 3, Number 10, 2008, pp. 30.

[7] Baltazar, H. “Are you prepared?” *eWeek*, Volume 8, Number 13, 2005, pp. 43-45.

[8] Beaman, B. and Albin, B. “Steps to disaster recovery planning,” *Network World*, Volume 25, 6, 2008, 25.

[9] Bowen, T. “Planning for recovery,” *Info World*, Volume 4, Number 8, 1999, pp. 83.

[10] Bradbury, C. “Disaster! Creating and testing an effective recovery plan,” *British Journal of Administrative Management*, Volume 23, Number 4, 2008, pp. 14-16.

[11] Brodkin, J. “When one data center is not enough,” *Network World*, Volume 25, Number 5, 2008, pp. 32.

[12] Buckley, M. “Calm during crisis,” *Health Management Technology*, Volume 8, Number 11, 2002, pp. 42-44.

[13] Budko, R. “Messaging disaster recovery – A necessity for disaster recovery,” *Government Procurement*, Volume 14, Number 10, 2007, pp. 30-31.

[14] Byrd, T., Turner, D. “Measuring the flexibility of information technology infrastructure: exploratory analysis of a construct,” *Journal of Management Information Systems*, Volume 17, Number 1, 2000, pp. 167-208.

[15] Chin, W. The Partial Least Squares Approach to Structural Equation Modeling. In Marcoulides, G. ed. *Modern Methods for Business Research*. Mahwah, NJ: Lawrence Erlbaum Associates, 1998, pp. 295-336.

[16] Connor, D. “Users assess plans for data protection, disaster recovery,” *Network World*, Volume 22, Number 10, 2005, pp. 10.

[17] Connor, D. “IT was prepared for Hurricane Rita,” *Network World*, Volume 22, Number 9, 2005, pp. 16.

[18] Cox, J. “The case of the great hot-swap site,” *Network World*, Volume 24, Number 30, 2007, pp. 42-45.

[19] Crowe, M. “Today’s disaster recovery: A holistic approach to remediation,” *Illinois Banker*, 43, Number 12, 2007, pp. 16-17.

[20] Curtis, G. “Beyond disaster recovery,” *Directorship*, Volume 23, Number 2, 2008, pp. 38-42.

[21] D’agostino, D. “Stormy weather,” *CIO*, Volume 19, Number 8, 2006, pp. 24.

[22] Davis, C. “Planning for the unthinkable: IT contingencies,” *International Education Journal*, Volume 21, Number 4, 2001, pp. 4-5.

[23] Defelice, A. “Preparing for the worst,” *Accounting Technology*, Volume 20, Number 4, 2008, pp. 14-19.

[24] Denyer, C. “Like the boy scouts, be prepared,” *Employee Benefit News*, Volume 19, Number 3, 2008, pp. 18-20.

[25] Diamantopoulos, A. and Winklhofer, H. “Index Construction with Formative Indicators: An Alternative to Scale Development.” *Journal of Marketing Research,* Volume 38, Number 2 2001, pp. 269-277.

[26] Drill, S. “Assume the worst in IT disaster recovery plan,” *National Underwriter*, Volume 32, Number 2, 2005, pp. 14-16.

[27] Farazmand, A. “Learning from the Katrina Crisis: A global and international perspective with implications for future crisis management,” *Public Administration Review*, Volume 67, Number 1, 2007, pp. 149-159.

[28] FitzGerald, J. Dennis, A. *Business data communications and networking*, 9th edition, Wiley, New York, 2005.

[29] Fonseca, B. “NY IT prepares for IT disaster recovery,” *eWeek*, Volume 7, Number 32, 2004, pp. 9-10.

[30] Gagnon, R. “When disasters strike,” *Mass Builder*, Volume 25, Number 3, 2008, pp. 21-22.

[31] Gale, S., Scott, R. “In for the long haul,” *PM Network*, Volume 19, Number 2, 2008, pp. 31-43.

[32] Giannacopoulos, P. “Paranoia is good,” *Strategic Finance*, Volume 32, Number 1, 2004, pp. 26-29.

[33] Gold, L. “Disaster recovery planning: How do you measure up?” *Accounting Today*, Volume 21, Number 7, 2007, pp. 31-35.

[34] Gold, L. “Security still tops tech concerns,” *Accounting Today*, Volume 22, Number 3, 2008, pp. 25-28.

[35] Green, R. “Peace of mind: Disaster recovery plans can keep your business alive,” *California CPA*, Volume 33, Number 2, 2005, pp. 23-24.

[36] Griffin, J. “Rental industry preps responds to hurricane disasters,” *Underground Construction*, Volume 8, Number 11, 2008, pp. 43-45.

[37] Grygo, E., Prencipe, L., Schwartz, E., Scannell, E., Krill, P. “IT recovery efforts forge ahead,” *Info World*, Volume 6, Number 9, 2001, pp. 17.

[38] Guster, D. McCann, B., Krzenski, K., Lee, O. “A cost effective, safe, and simple method to provide a disaster recovery plan to small and medium businesses,” *Review of Business Research*, Volume 8, Number 4, 2008, pp. 63-71.

[39] Hall, M. “On the Mark,” *Computer World*, Volume 21, Number 11, 2007, pp. 20.

[40] Harney, “Business continuity and disaster recovery: Backup or shutdown,” *eDoc Magazine*, Volume 3, Number 3, 2004, pp. 42-43.

[41] Havenstein, H., Fisher, S., Thibodeau, P. “IT execs race against time along Gulf coast,” *Computer World*, Volume 40, Number 6, 2006, pp. 7.

[42] Hayes, J. “Reaping the whirlwind,” *IEE Review*, Volume 13, Number 3, 2005, pp. 29.

[43] Hoge, J. “Business continuity planning must extend to vendors,” *Bank Technology News*, Volume 11, Number 3, 2005, pp. 21.

[44] Holliday, K. “Planning for the worst,” *Community Banker*, Volume 22, Number 8, 2008, pp. 32-35.

[45] Hoovers, Inc. “Computer fact sheets,” Retrieved July 27, 2009 from Hoover’s Online Pro Plus database, 2006.

[46] Hurdis, B. “Disaster recovery and business continuity planning: A strategic investment,” *Illinois Banker*, Volume 44, Number 3, 2008, pp. 10-11.

[47] Jackson, R. “In times of crisis,” *Internal Auditor*, Volume 31, Number 4, 2008, pp. 46-51.

[48] Jarvis, C., Mackenzie, S, Podsakoff, P. and Mick, D. A “Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research.” *Journal of Consumer Research,* Volume 30, Number 2 2003, pp. 199-218.

[49] Jepson, K. “How 1 small CU perfected its own recipe for disaster recovery,” *Credit Union Journal*, Volume 23, Number 9, 2008, pp. 20.

[50] Kepczyk, R. “In-firm view of the AICPA top technology initiatives,” *CPA Technology Advisor*, Volume 18, Number 3, 2008, pp. 46-47.

[51] Kim, Y. “Validation of psychometric research instruments: The case of information science,” *Journal of the American Society for Information Science & Technology*, Volume 60, Number 6, 2009, pp. 1178-1191.

[52] Krippendorff, K. *Content analysis: An introduction to its methodology*, Sage, London, 1980.

[53] Kumar, R., Park, S., Subramaniam, C. “Understanding the value of countermeasure portfolios in information system security,” *Journal of Management Information Systems*, Volume 25, Number 2, 2008, pp. 241-279.

[54] Laliberte, B. “How disaster-tolerant is your company,” *Business Communications Review*, Volume 32, Number 4, 2007, pp. 44-49.

[55] Landa, H. “Planning for disaster,” *Associations Now*, Volume 11, Number 3, 2008, pp. 21-22.

[56] Lanter, A. “Staying ahead of the disaster recovery plan: Requirements are changing at record speeds,” *Illinois Banker*, 44, Number 4, 2008, pp. 6-8.

[57] Lawshe, C. “A quantitative approach to content validity,” *Personnel Psychology*, Volume 28, Number 4, 1975, pp. 563-575.

[58] Lewis B., Templeton, G., Byrd, T. “A methodology for construct development in MIS research.” European Journal of Information Systems, Volume 14, Number 2, 2005, pp. 388-400.

[59] Lindstedt, D. “Grounding the discipline of business continuity planning: What needs to be done to take it forward?” *Journal of Business Continuity & Emergency Planning*, Volume 2, Number 2, 2007, pp. 197-205.

[60] Lin, A., Gregor, S., Ewing, M. “Developing a scale to measure the enjoyment of web experiences,” *Journal of Interactive Marketing*, Volume 22, Number 2, 2008, pp. 40-57.

[61] Lohrman, D. “Disaster Recovery: A process – not a destination,” *Public CIO*, Volume 8, Number 2, 2007, pp. 54.

[62] Lundequist, E. “Disaster plans tied to business success,” *eWeek*, Volume 4, Number 5, 2001, pp. 3.

[63] Malhotra, M., Grover, V. “An assessment of survey research in POM: From constructs to theory,” *Journal of Operations Management*, Volume 16, Number 4, 1998, pp. 403-423.

[64] Marakas, G., Johnson, R. and Clay, P. “Formative vs. Reflective Measurement: A reply to Hardin, Chang, and Fuller.” *Journal of the Association for Information Systems* Volume 9, Number 9 2008, pp. 535-543.

[65] McLaughlin, L. “Rethinking disaster recovery,” *CIO*, Volume 21, Number 6, 2008, pp. 23-26.

[66] Mearian L. “Key financial firms compare notes on disaster recovery,” *Computer World*, Volume 38, Number 31, 2004, pp. 43.

[67] Mearian, L. “Users are rethinking disaster recovery plans,” *Computer World*, Volume 39, Number 36, 2005, pp. 8.

[68] Mearian, L. “Hurricane, floods, put IT staff to the test,” *Computer World*, Volume 39, Number 36, 2005, pp. 4.

[69] Mearian, L. “IT execs must fight for disaster recovery money,” *Computer World*, Volume 39, Number 35, 2005, pp. 19.

[70] Mearian L., Weiss, T. “Lessons learned, IT managers steel for Rita,” *Computer World*, Volume 39, Number 4, 2005, pp. 66.

[71] Pabrai, U. “Contingency planning and disaster recovery,” *Certification Magazine*, Volume 5, Number 8, 2004, pp. 38-39.

[72] Petter, S., Petter, S., Straub, D. and Rai, A. “Specifying formative constructs in information systems research.” *MIS Quarterly,* Volume 31, Number 4 2007, pp. 623-656.

[73] Plotnick, N. “When disaster plans fall short,” *PC Week*, Volume 28, Number 2, 1999, pp. 58.

[74] Postal, A. “Disaster recovery plan seen as critical to GEB’s survival,” *National Underwriter*, Volume 35, Number 4, 2007, pp. 23-25.

[75] Pregmon, M. “IT disaster recovery planning: Are you up and ready? Part 1: Risk analysis,” *Journal of the Quality Assurance Institute*, Volume 27, Number 2, 2007, pp. 23-24.

[76] Pregmon, M. “IT disaster recovery planning: Are you up and ready? Part 2: Internal Control,” *Journal of the Quality Assurance Institute*, Volume 27, Number 3, 2007, pp. 25-28.

[77] Pregmon, M. “IT disaster recovery planning: Are you up and ready? Part 3: The recovery planning process,” *Journal of the Quality Assurance Institute*, Volume 27, Number 4, 2007, pp. 10-12.

[78] Pregmon, M. “IT disaster recovery planning: Are you up and ready? Part 4: IT virtualization,” *Journal of the Quality Assurance Institute*, Volume 28, Number 1, 2008, pp. 26-27.

[79] Preimesberger, C. “On the brink of disaster,” *eWeek*, Volume 11, Number 2, 2008, pp. 31-38.

[80] Price, E. “The new scope of business continuity,” *eDoc Magazine*, Volume 3, Number 4, 2004, pp. 34-35.

[81] Ramsaran, C. “Running ahead of the pack,” *Bank Systems & Technology*, Volume 1, Number 4, 2005, pp. 1-3.

[82] Retelle, M. “Plan for disaster,” *Credit Union Magazine*, Volume 21, Number 9, 2008, pp. 80.

[83] Rolich, P. “Setting priorities: Business continuity from an IT perspective – is it better to be right or liked?” *Tech Decisions*, Volume 9, Number 2, 2008, pp. 11-14.

[84] Saccomanno, P., Mangialardi, V. “Be prepared for IT disasters,” *Canadian Consulting Engineer*, Volume 32, Number 4, 2008, pp. 35-40.

[85] Sheth, S., McHugh J., Jones, F. “A dashboard for measuring capability when designing, implementing and validating business continuity and disaster recovery projects,” *Journal of Business Continuity & Emergency Planning*, Volume 2, Number 3, 2008, pp. 221-239.

[86] Sliwa, C. “Retailers unsure about the status of stores, systems,” *Computer World*, Volume 39, Number 3, 2005, pp. 5.

[87] Sliwa, C. “Marriott goes underground with disaster recovery,” *CIO*, Volume 13, Number 8, 2008, pp. 44-46.

[88] Snow, C. “Can’t stop, won’t stop,” *American City and County*, Volume 4, Number 11, 2008, pp. 26.

[89] Stemler, S. “An overview of content analysis,” *Practical Assessment, Research, & Evaluation*, Volume 17, Number 2, 2001, pp. 23-42.

[90] Stoller, J. “Contemplating the unthinkable – disaster recovery and the Canadian business environment,” *CMA Management*, Volume 37, Number 3, 2008, pp. 48-49.

[91] Sturdevant, C. “A business plan to survive the big one, *eWeek*, Volume 4, Number 8, 2001, pp. 70.

[92] Sullivan, B. “Many communities wrestling with explosive growth, long-term problems,” *MSBNC Reports*, retrieved from http://www.msnbc.msn.com/id/14542913/page/1/ on July 27, 2009.

[93] Symantec, “State of the data center regional data – Global,” Second annual report, Cupertino, CA, 2008.

[94] Templeton, G. Lewis, B., Snyder, C. “Development of a measure for the organizational learning construct,” *Journal of Management Information Systems*, Volume 19, Number 2, 2002, pp. 175-218.

[95] Thibodeau, P., Mearian, L. “Users start to weigh long-term IT issues,” *Computer World*, Volume 39, Number 37, 2005, pp. 61-67.

[96] Tojib, D., Sugianto, L., Sendjaya, S. “User satisfaction with business-to-employee portals: conceptualization and scale development,” *European Journal of Information Systems*, Volume 17, Number 6, 2008, pp. 649-667.

[97] Tueros, M. “When disaster strikes,” *Smart Business Miami*, Volume 6, Number 2, 2008, pp. 18.

[98] Vessey, I., Ramesh, V., Glass, R. “Research in information systems: An empirical study of diversity in the discipline and its journals,” *Journal of Management Information Systems*, Volume 19, Number 2, 2002, pp. 129-174.

[99] Vigdor, J. “The economic aftermath of Hurricane Katrina,” *Journal of Economic Perspectives*, Volume 22, Number 4, 2008, pp. 135-154.

[100] Vijayan, J. “Data security risks missing from disaster recovery plans,” *Computer World*, Volume 39, Number 41, 2005, pp. 16-18.

[101] Wang, C., Ahmed, P., Rafiq, M. “Knowledge management orientation: construct development and empirical orientation, *European Journal of Information Systems*,” Volume 17, Number 3, 2008, pp. 219-235.

[102] Weber, R. “*Basic content analysis*,” Sage, London, 1985.

[103] Weiss, T. “Gustav finds IT execs prepared for the worst,” *Computer World*, Volume 42, Number 32, 2008, pp. 4.

[104] Wild R., Griggs, K., Li, E. "An architecture for distributed scenario building and evaluation," *Communications of the ACM*, Volume 48, Number 11, 2005, pp. 80-86.

[105] Zalud, B. "Continuity behind the lines," *Security*, Volume 4, Number 2, 2008, pp. 108.

AUTHOR BIOGRAPHIES

Dr. Christopher Kadlec is an assistant professor of information technology at Georgia Southern University. He has 17 years experience in IT management and has taught IT courses for 10 years. He completed his doctorate at the Terry College of Business Administration, University of Georgia. His research interests are in IT disaster recovery planning, self-regulated learning, power users of IT, and networking. His work has been published in multiple journal and conference proceedings.

Dr. Jordan Shropshire is an assistant professor of information technology at Georgia Southern University. His research interests focus on the behavioral and technical aspects of information security, IT disaster recovery planning, networking, and infrastructure management. He recently completed his dissertation on information security at Mississippi State University. He is the author of multiple journal articles and conference proceedings. He has served as an associate editor and/or reviewer for leading journals, including MIS Quarterly, European Journal of Information Systems, Information & Organization, and Journal of Information Systems Security.

APPENDIX A: ARTICLES INCLUDED IN CONTENT ANALYSIS

The following articles were included in the content analysis:

Anderson, 2008
Anthes, 2008
April and Gryco, 2008
Ashton, 2008
Baker, 2008
Baltazar, 2005
Beaman and Albin, 2008
Bowen, 1999
Brodkin, 2008
Buckley, 2002
Budko, 2007
Connor, 2005a
Connor, 2005b
Cox, 2007
Crowe, 2007
Curtis, 2008
D'agostino, 2006
Davis, 2001
Defelice, 2008
Denyer, 2008
Drill, 2005
Fonseca, 2004
Gagnon, 2008
Gale, and Scott, 2008
Giannacopoulos, 2004
Gold, 2007
Gold, 2008
Green, 2005
Griffin, 2008
Grygo, et al., 2001
Guster, et al., 2008
Hall, M. (2007
Harney, (2004
Havenstein, et al., 2006
Hayes, 2005
Hoge, 2005
Holliday, 2008
Hurdis, 2008
Jackson, 2008
Jepson, 2008
Kepczyk, 2008
Kumar, et al., 2008
Laliberte, 2007
Landa, 2008
Lanter, 2008
Lindstedt, 2007
Lohrman, 2007
Lundequist, 2001
McLaughlin, 2008
Mearian 2004
Mearian, 2005a
Mearian, 2005b
Mearian, 2005c
Mearian and Weiss, 2005
Pabrai, 2004
Patel, 2003
Plotnick, 1999
Postal, 2007
Pregmon, 2007a
Pregmon, 2007b
Pregmon, 2007c
Pregmon, 2008
Preimesberger, 2008
Ramsaran, 2005
Retelle, 2008
Rolich, 2008
Saccomanno and Mangialardi, 2008
Sheth, et al., 2008
Sliwa, 2005
Sliwa, 2008
Snow, 2008
Stoller, 2008
Sturdevant, 2001
Thibodeau, and Mearian, 2005
Tueros, 2008
Vijayan, 2005
Weiss, 2008
Wild and Griggs, 2005
Zalud, 2008

APPENDIX B: CODING SCHEMES

Initial coding scheme, adopted from Fitzgerald and Dennis [28]:

- The name of the decision-making manager who is in charge of the disaster recovery operation; a second manager should be indicated in case the first manager is unavailable.
- Staff Assignments and responsibilities during the disaster
- A pre-established list of priorities that states what is to be fixed first
- Location of alternative facilities operated by the company or a professional disaster recovery firm and procedures for switching operations to those facilities using backups of data and software
- Recovery procedures for the data communication facilities (backbone network, metropolitan area network, wide area network, and local area network), servers, and application systems; this includes information on the location of circuits and devices, whom to contact for information, and the support that can be expected from vendors, along with the name and telephone number of the person at each vendor to contact
- Action to be taken in case of partial damage or threats such as bomb threats, fire, water or electrical damage, sabotage, civil disorders, and vendor failures
- Manual processes to be used until the network is functional
- Procedures to ensure adequate updating and testing of the disaster recovery plan
- Storage of the data, software, and the disaster recovery plan itself in a safe area where they cannot be destroyed by a catastrophe. This area must be accessible, however, to those who need to use the plan

Final coding scheme:

- Procedures for detecting IT disasters
- Procedures for informing IT disaster recovery team members that an IT disaster has occurred
- Procedures for informing stakeholders that an IT disaster has occurred
- Establishment or formalization of communication channels to be used in the event of an emergency
- Formalization of a decision making structure
- Staff assignments and responsibilities during the disaster
- Training and briefing of personnel in the event of a disaster
- Identification of IT services
- Identification of risks to IT services and infrastructure
- Listing of the order in which services need to be reactivated
- Alternative facilities and procedures for switching operations to those facilities
- Recovery procedures for service inputs such as human resources
- Recovery procedures for service inputs such as facilities
- Recovery procedures for service inputs such as communications technologies
- Recovery procedures for service inputs such as servers
- Recovery procedures for service inputs such as application systems
- Recovery procedures for service inputs such as data
- Backup copies of data
- Backup copies of software
- Backup copies of configuration files
- Backup copies of the IT disaster recovery plan
- Offsite locations to backup data
- Offsite locations to backup software
- Offsite locations to backup configuration files
- Offsite locations to backup the IT disaster recovery plan
- Measures for ensuring that systems, software, and data are as portable as possible
- Documentation of configuration and changes to systems, hardware, software
- Procedures to ensure adequate testing of the disaster recovery plan
- Procedures to ensure continual updating disaster recovery plans
- Procedures to ensure the IT disaster recovery plan is part of the business continuity plan

APPENDIX C: ORIGINAL ITEMS FOR OPERATIONALIZING ITDR

- We have procedures for detecting incidents
- We have procedures for classifying incidents as disasters
- We have a means of assessing the magnitude of IT disasters
- We have procedures for alerting individuals responsible for IT disaster recovery
- We have procedures for letting stakeholders know that an IT disaster has occurred
- We have established an alternative means of communications (i.e. cell phones) to use in emergencies
- We have designated an individual to restart data processing systems following disaster
- We have designated an individual to restore communications following disaster
- We have designated an individual to restore data following disaster
- We have designated an individual to restore supporting infrastructure following disaster
- We have designated an individual to lead operations following disaster
- Those responsible for IT disaster recovery have been assigned specific tasks for restoring IT services
- Employees and other stakeholders know what to expect during IT disasters
- We have selected an IT governance structure to implement following IT disaster
- We have an explicit chain of command for dealing with IT disasters
- We have identified all IT services which the IT department offers
- We have audited the inputs of all IT services
- We have identified all system resources required to provide IT services
- We have assessed risks to IT services and infrastructure
- We have ranked the order in which IT services would be repaired, if a disaster occurred
- Should our primary site go offline, we have a secondary site
- Should our primary site go offline, we have procedures for relocating IT operations
- Our plans account for missing IT workers
- Our plans account for incapacitated IT workers
- Our plans account for possible losses of human resources (i.e. missing or injured IT workers)
- We have procedures for restoring physical IT infrastructure
- We have procedures for restoring physical supporting infrastructure
- We have procedures for recovering communications technologies such cellular phones, email, and VOIP
- We have procedures for recovering servers
- We have procedures for recovering operating systems
- We have procedures for recovering applications
- We have procedures for recovering information systems
- We have procedures for recovering data
- We have procedures for recovering configuration files, change logs, and other documents
- We have procedures for creating backup copies of data
- We have procedures for creating backup copies of operating systems
- We have procedures for creating backup copies of applications
- We have procedures for creating backup copies of information systems
- We have procedures for creating backup copies of configuration files, change logs, and other documents
- We have procedures for creating backup copies of the disaster recovery plan itself
- We have ensured that system resources are as portable as possible (i.e. that they can be transported)
- We have offsite locations for storing data
- We have offsite locations for storing software
- We have offsite locations for storing configuration files, change logs, and other relevant documents
- We have offsite locations for storing copies of the IT disaster recovery plan
- We have hot sites ready for immediate use
- We have warm sites which can be quickly brought online
- We have cold sites which require start up
- We have procedures for testing of the IT disaster recovery plan
- We have procedures for updating the IT disaster recovery plan
- We have procedures for ensuring that the IT disaster recovery plan is part of the business continuity plan
- We have procedures for documenting system configurations, changes, and updates

APPENDIX D: SURVEY INSTRUCTIONS

Survey instructions found on both paper and online versions:

The purpose of this assessment is to measure the degree to which your organization conducts IT disaster recovery planning. We define IT disaster recovery planning as the set of actions (IT disaster identification and notification, preparing organizational members, IT services analysis, recovery process, backup procedures, offsite storage, and maintenance) which an organization follows in order to improve its ability to resume IT services following a disaster.

There are 45 questions in this survey

Please complete this portion of the survey on behalf of your organization. Rate the degree to which you agree or disagree with each of the following items.