2009

Establishing the IT Disaster Recovery Planning Construct

Christopher Kadlec
Georgia Southern University, ckadlec@georgiasouthern.edu

Jordan Shropshire
Georgia Southern University, jshropshire@georgiasouthern.edu

Americas Conference on Information Systems
AMCIS2009 San Francisco

Establishing the IT Disaster Recovery Planning Construct

Christopher Kadlec
Georgia Southern University
ckadlec@georgiasouthern.edu

Jordan Shropshire
Georgia Southern University
jshropshire@georgiasouthern.edu

ABSTRACT (REQUIRED)

The concept of IT disaster recovery planning is receiving an increasing amount of attention from IT practitioners and business managers due to its importance in averting disasters and ensuring the continuity of organizations. Surprisingly, little research has been aimed at providing a comprehensive definition of this topic. Thus, this manuscript describes the process by which conceptual definition of IT disaster recovery planning is developed and an exhaustive listing of the construct's dimensions is derived via content analysis. In this meta-study, 72 articles were found to yield 572 individual planning recommentations related to IT disaster recovery planning. The data were analyzed using a clustering technique and formed into 7 dimensions and 16 sub-dimensions. The results can be used to guide organizations' IT disaster recovery planning processes.

Keywords (Required)

IT disaster recovery planning, domain definition, content analysis, measurement

INTRODUCTION

Organizations have become more reliant on information technology (IT) which is becoming integrated into all parts of those organizations. This puts greater emphasis on the IT professional to keep the services provided by the technology working. In the U.S., regulations such as Sarbanes-Oxley and HIPAA require some organizations have a disaster recovery plan. In light of these government regulations and the importance of IT to organizations, 28% of IT executives either do not know what their plan to continue is or know they do not have one (AT&T Global Reports, 2008). For those organizations that have full scale data centers, 22% respond that their plan needs work (Symantec, 2008). These two surveys leave out the organizations that do not have a "IT Executive" or a "Data Center."

While Information Technology Disaster Recovery Planning (ITDRP) is included in IS/IT textbooks (Fitzgerald and Dennis, 2005), is cited as important in IS/IT literature (Guster, Krzenski & Lee, 2008; Kumar, Park & Subramaniam, 2008; Ramsaran, 2005), and described in practitioner journals (See Apendix B), neither a conceptual definition nor a process for the practitioner to follow has been offered by IS/IT literature. Thus, the purpose of this paper is to introduce a conceptual definition of IT Disaster Recovery Planning and the actions that make up the planning process.

The definition is derived using content analysis. An a priori coding scheme, based on the work of Fitzgerald and Dennis (2005), was developed. Some 72 practitioner and academic articles, found in the Pro-Quest and Business Source Complete databases, were coded. Using the data cluster technique described by Krippendorff (1980), a conceptual definition was formed. As a result, ITDRP is defined as the set of actions which an organization follows in order to improve its ability to resume IT services following a disaster. The actions that an organization would follow, discussed in more depth later, are IT disaster identification and notification, preparing organizational members, IT services analysis, recovery process, backup procedures, offsite storage, and maintenance.

DEFINING THE IT DISASTER RECOVERY PLANNING DOMAIN

Historically, IT disaster recovery planning had a rather simplistic meaning; it was generally limited to backing up data and devising methods to restore data resources. With the integration of IT into all business functions and the reliance on technology among organizational members, the complexity of IT disaster recovery planning significantly escalates. There is little guidance in IS/IT literature for the practitioner to develop and maintain an IT disaster recovery plan. Existing guidance is often incomplete on its own and inconsistent with other parts of the literature.

One area that has been confused in the literature is the difference between "IT disaster recovery" and "business continuity". Business continuity planning address how an organization is to continue as an entity into the future, and is therefore a superset of IT Disaster Recovery. Business continuity planning is from the viewpoint of the organization and does not offer direct guidance to the IT professional. The ITDRP must be written to not conflict with the business continuity plan and must not allow the IT to sub-optimize as it is restored after the IT disaster.

Another area of confusion is what constitutes an IT disaster. IT disasters impact the organization in which the IT service is employed. IT disasters range from the accidental deletion of a file to a hurricane that destroys the building that houses the data center along with the infrastructure (such as electrical power grid) in the area of the data center. 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. The loss of inputs leads to disaster only if it causes a failure in the associated IT services.

IT disaster recovery plans are for restoring IT services, not necessarily for restoring specific hardware and software architectures. It may not be possible, feasible, or practical to return to pre-disaster conditions. Disaster recovery for a service is complete when the service has been brought back online and is considered sustainable.

ITDRP does not involve simplification of IT services. The purpose of ITDRP is not to simplify IT services so that they are easier to restore, but to devise alternate ways of restoring IT services. When an organization evacuates the fit and function of the IT infrastructure while preparing an IT disaster plan, it is not prescribed that the underlying infrastructure should be simplified so as to make recovery easier. The IT services should be evaluated prior to the ITDRP process as to whether they should continue or not. Additionally, avoiding a disaster is not planning a way of planning to recovery from a disaster but disaster mitigation.

ITDRP requires an in-depth understanding of the IT services offered in terms of: 1) how the technology works 2) how the technology is configured and 3) how that system is used within the organization. Without the knowledge of all three domains, a service may not be brought back to provide the functionality that was once there. Unfortunately, the extant literature lacks a comprehensive definition which could help organizations address these issues.

This meta-study looks at the available literature and gives seven dimensions of IT disaster recovery planning and sixteen sub-dimensions that will help define for research and practice the areas that an IT disaster recovery plan should address. This will help guide future research but also guide practice to build highly reliable systems by providing a framework for the IT disaster recovery plan.

METHOD

The purpose of this analysis is to develop a conceptual definition of IT disaster recovery planning, including a comprehensive list of the dimensions which represent the elements of the construct. The technique used to derive this artifact is content analysis. Content analysis is a research method used in the social sciences to draw inferences from text (Weber, 1985). 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 investigators independently coded each reference unit, and later convened to compare results. The initial level of agreement was approximately 85% of cases. In cases of disagreement, the researchers collectively reviewed the attributes of reference units until a consensus was reached. Over 98% of coding disputes were resolved in this manner. An independent IT professional was asked to judge the remaining cases. 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 (e.g. Byrd and Turner, 2000; Lewis *et al.,* 2005; Templeton *et al.*, 2002).

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 in 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 B). It should be noted that the majority of the articles were published in trade publications, industry-specific magazines, and IT practitioner–oriented journals; few 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 (Krippendorf, 1980).

Coding Scheme

An a priori coding scheme was used to categorize the data (Stemler, 2001). The coding scheme was initially based on a list of 9 elements of an IT disaster recovery plan (Fitzgerald and Dennis, 2005) (see Appendix A). 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 A). This method has been advocated by qualitative researchers such as Weber (1990). Although the process of decoding 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 sub-dimensions. As with coding, clustering is a qualitative research technique. Thus, the most rigorous method of clustering was used (Krippendorff, 1980). 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. Because the definition is independent of specific technologies, IT architectures, and organizational governance schemes, it can be applied to a wide range of organizations.

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 creating backup copies of data, software, configuration files, and the IT disaster recovery plan.	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.

Table 1. Dimensions of the IT Disaster Recovery Planning Construct

CONCLUSION

This research represents one of the first efforts at providing a systematically-developed definition of IT disaster recovery planning. A limitation of the current study is that it relied heavily on trade literature. This limitation is an extension of the cited need for this study; little research has been aimed at providing a comprehensive definition of the topic of IT disaster recovery planning. Future research should focus on the refinement of this definition. For instance, incorporating feedback from representative practitioner groups and conducting empirical evaluations will provide subsequent improvements to the current conceptualization. Additional research should aim at developing a measure for this construct, so that it may be incorporated in further research. Despite the need for additional attention, the current 7 dimension, 16 sub-dimension construct is a considerable advancement for an under-studied field. The results can not only guide future research but practitioners as they try to guard their organizations against disaster.

REFERENCES

1. Anderson, J. (2008) New trends in backup: Is your disaster recovery plan keeping up? *The eSecurity Advisor*, 8, 2, 58.
2. Anthes, G. (2008) Apocalypse Soon, *Computer World,* 42, 23, 24-28.
3. April, C. and Gryco, E. (2001) Users fortifying enterprise walls, *InfoWorld*, 6, 10, 17-20.
4. Ashton, H. (2008) How prepared is your business for a calamity? *Japan Inc*, 12, 1, 15-17.
5. AT&T (2008) Business continuity survey: 2008, AT&T Reports, Dallas.
6. Baker, S. (2008) Lessons learned: A devastating hurricane caused this CIO to rethink his carrier's disaster recovery plans, *Tech Decisions*, 3, 10, 30.
7. Baltazar, H. (2005) Are you prepared? *eWeek*, 8, 13, 43-45.
8. Beaman, B. and Albin, B. (2008) Steps to disaster recovery planning, *Network World*, 25, 6, 25.
9. Bowen, T. (1999) Planning for recovery, *Info World*, 4, 8, 83.
10. Bradbury, C. (2008) Disaster! Creating and testing an effective recovery plan, *British Journal of Administrative Management*, 23, 4, 14-16.
11. Brodkin, J. (2008) When one data center is not enough, *Network World*, 25, 5, 32.
12. Buckley, M. (2002) Calm during crisis, *Health Management Technology*, 8, 11, 42-44.
13. Budko, R. (2007) Messaging disaster recovery – A necessity for disaster recovery, *Government Procurement*, 14, 10, 30-31.
14. Byrd, T., Turner, D. (2000) Measuring the flexibility of information technology infrastructure: exploratory analysis of a construct, *Journal of Management Information Systems*, 17, 1, 167-208.
15. Chisholm, P. (2008) Disaster recovery planning is business critical, *the CPA Journal*, 21, 7, 11.
16. Connor, D. (2005) Users assess plans for data protection, disaster recovery, *Network World*, 22, 10, 10.
17. Connor, D. (2005) IT was prepared for Hurricane Rita, *Network World*, 22, 9, 16.
18. Cox, J. (2007) The case of the great hot-swap site, *Network World*, 24, 30, 42-45.
19. Crowe, M. (2007) Today's disaster recovery: A holistic approach to remediation, *Illinois Banker*, 43, 12, 16-17.
20. Curtis, G. (2008) Beyond disaster recovery, *Directorship*, 23, 2, 3838-42.
21. D'agostino, D. (2006) Stormy weather, *CIO*, 19, 8, 24.
22. Davis, C. (2001) Planning for the unthinkable: IT contingencies, *International Education Journal*, 21, 4, 4-5.
23. Defelice, A. (2008) Preparing for the worst, *Accounting Technology*, 20, 4, 14-19.
24. Denyer, C. (2008) Like the boy scouts, be prepared, *Employee Benefit News*, 19, 3, 18-20.
25. Dignan, L. (2004) Pop culture, *Baseline*, 13, 47, 18.

26. Drill, S. (2005) Assume the worst in IT disaster recovery plan, *National Underwriter*, 32, 2, 14-16.
27. FitzGerald, J. Dennis, A. (2005) Business data communications and networking, 9th edition, Wiley, New York.
28. Fonseca, B. (2004) NY IT prepares for IT disaster recovery, *eWeek*, 7, 32, 9-10.
29. Gagnon, R. (2008) When disasters strike, *Mass Builder*, 25, 3, 21-22.
30. Gale, S. and Scott, R. (2008) In for the long haul, *PM Network*, 19, 2, 31-43.
31. Giannacopoulos, P. (2004) Paranoia is good, *Strategic Finance*, 32, 1, 26-29.
32. Gold, L. (2007) Disaster recovery planning: How do you measure up? *Accounting Today*, 21, 7, 31-35.
33. Gold, L. (2008) Security still tops tech concerns, *Accounting Today*, 22, 3, 25-28.
34. Green, R. (2005) Peace of mind: Disaster recovery plans can keep your business alive, *California CPA*, 33, 2, 23-24.
35. Griffin, J. (2008) Rental industry preps responds to hurricane disasters, *Underground Construction*, 8, 11, 43-45.
36. Grygo, E., Prencipe, L., Schwartz, E., Scannell, E., Krill, P. (2001) IT recovery efforts forge ahead, *Info World*, 6, 9, 17.
37. Guster, D. McCann, B., Krzenski, K., Lee, O. (2008) A cost effective, safe, and simple method to provide a disaster recovery plan to small and medium businesses, *Review of Business Research*, 8, 4, 63-71.
38. Hall, M. (2007) On the Mark, *Computer World*, 21, 11, 20.
39. Harney, (2004) Business continuity and disaster recovery: Backup or shutdown, *eDoc Magazine*, 3, 3, 42-43.
40. Havenstein, H., Fisher, S., Thibodeau, P. (2006) IT execs race against time along Gulf coast, *Computer World*, 40, 6, 7.
41. Hayes, J. (2005) Reaping the whirlwind, *IEE Review*, 13, 3, 29.
42. Hoge, J. (2005) Business continuity planning must extend to vendors, *Bank Technology News*, 11, 3, 21.
43. Holliday, K. (2008) Planning for the worst, *Community Banker*, 22, 8, 32-35.
44. Hurdis, B. (2008) Disaster recovery and business continuity planning: A strategic investment, *Illinois Banker*, 44, 3, 10-11.
45. Jackson, R. (2008) In times of crisis, *Internal Auditor*, 31, 4, 46-51.
46. Jaques, M. (2006) Securing your IT continuity, *Financial Director*, 28, 7, 42.
47. Jepson, K. (2008) How 1 small CU perfected its own recipe for disaster recovery, *Credit Union Journal*, 23, 9, 20.
48. Kepczyk, R. (2008) In-firm view of the AICPA top technology initiatives, *CPA Technology Advisor*, 18, 3, 46-47.
49. Krippendorff, K. (1980) Content analysis: An introduction to its methodology, Sage, London.
50. Kumar, R., Park, S., Subramaniam, C. (2008) Understanding the value of countermeasure portfolios in information system security, *Journal of Management Information Systems*, 25, 2, 241-279.
51. Laliberte, B. (2007) How disaster-tolerant is your company, *Business Communications Review*, 32, 4, 44-49.
52. Landa, H. (2008) Planning for disaster, *Associations Now*, 11, 3, 21-22.
53. Lanter, A. (2008) Staying ahead of the disaster recovery plan: Requirements are changing at record speeds, *Illinois Banker*, 44, 4, 6-8.
54. Lewis B., Templeton, G., Byrd, T. (2004) A methodology for construct development in MIS research. European Journal of Information Systems, 14, 2, 388-400.
55. Lindstedt, D. (2007) Grounding the discipline of business continuity planning: What needs to be done to take it forward? *Journal of Business Continuity & Emergency Planning*, 2, 2, 197-205.
56. Lohrman, D. (2007) Disaster Recovery: A process – not a destination, *Public CIO*, 8, 2, 54.
57. Lundequist, E. (2001) Disaster plans tied to business success, *eWeek*, 4, 5, 3.
58. McAdams, J. (2008) Highlight: Hardrock hotel and casino, *Computer World*, 42, 23, 35.

59. McLaughlin, L. (2008) Rethinking disaster recovery, *CIO*, 21, 6, 23-26.
60. Mearian L. (2004) Key financial firms compare notes on disaster recovery, *Computer World*, 38, 31, 43.
61. Mearian, L. (2005) Users are rethinking disaster recovery plans, *Computer World*, 39, 36, 8.
62. Mearian, L. (2005) Hurricane, floods, put IT staff to the test, *Computer World*, 39, 36, 4.
63. Mearian, L. (2005) IT execs must fight for disaster recovery money, *Computer World*, 39, 35, 19.
64. Mearian L., Weiss, T. (2005) lessons learned, IT managers steel for Rita, *Computer World*, 39, 39, 66.
65. Pabrai, U. (2004) Contingency planning and disaster recovery, *Certification Magazine*, 5, 8, 38-39.
66. Patel, R. (2003) Disaster recovery planning, *Automotive Industries*, 42, 23, 46-47.
67. Plotnick, N. (1999) When disaster plans fall short, *PC Week*, 28, 2, 58.
68. Postal, A. (2007) Disaster recovery plan seen as critical to GEB's survival, *National Underwriter*, 35, 4, 23-25.
69. Pregmon, M. (2007) IT disaster recovery planning: Are you up and ready? Part 1: Risk analysis, *Journal of the Quality Assurance Institute*, 27, 2, 23-24.
70. Pregmon, M. (2007) IT disaster recovery planning: Are you up and ready? Part 2: Internal Control, *Journal of the Quality Assurance Institute*, 27, 3, 25-28.
71. Pregmon, M. (2007) IT disaster recovery planning: Are you up and ready? Part 3: The recovery planning process, *Journal of the Quality Assurance Institute*, 27, 4, 10-12.
72. Pregmon, M. (2008) IT disaster recovery planning: Are you up and ready? Part 4: IT virtualization, *Journal of the Quality Assurance Institute*, 28, 1, 26-27.
73. Preimesberger, C. (2008) On the brink of disaster, *eWeek*, 11, 2, 31-38.
74. Price, E. (2004) The new scope of business continuity, *eDoc Magazine*, 3, 4, 34-35.
75. Ramsaran, C. (2005) Running ahead of the pack, *Bank Systems & Technology*, 1, 4, 1-3.
76. Retelle, M. (2008) Plan for disaster, *Credit Union Magazine*, 21, 9, 80.
77. Rolich, P. (2008) Setting priorities: Business continuity from an IT perspective – is it better to be right or liked? *Tech Decisions*, 9, 2, 11-14.
78. Saccomanno, P., Mangialardi, V. (2008) Be prepared for IT disasters, *Canadian Consulting Engineer*, 32, 4, 35-40.
79. Sheth, S., McHugh J., Jones, F. (2008) A dashboard for measuring capability when designing, implementing and validating business continuity and disaster recovery projects, *Journal of Business Continuity & Emergency Planning*, 2, 3, 221-239.
80. Sliwa, C. (2005) Retailers unsure about the status of stores, systems, *Computer World*, 39, 3, 5.
81. Sliwa, C. (2008) Marriott goes underground with disaster recovery, *CIO*, 13, 8, 44-46.
82. Snow, C. (2008) Can't stop, won't stop, *American City and County*, 4, 11, 26.
83. Stemler, S. (2001) An overview of content analysis, *Practical Assessment, Research, & Evaluation*, 17, 2, 23-42.
84. Stoller, J. (2008) Contemplating the unthinkable – disaster recovery and the Canadian business environment, *CMA Management*, 37, 3, 48-49.
85. Sturdevant, C. (2001) A business plan to survive the big one, *eWeek*, 4, 8, 70.
86. Symantec, (2008) State of the data center regional data – Global, Second annual report, Cupertino, CA.
87. Templeton, G. Lewis, B., Snyder, C. (2002) Development of a measure for the organizational learning construct, *Journal of Management Information Systems*, 19, 2, 175-218.
88. Thibodeau, P., Mearian, L. (2005) Users start to weigh long-term IT issues, *Computer World*, 39, 37, 61-67.
89. Tueros, M. (2008) When disaster strikes, *Smart Business Miami*, 6, 2, 18.

90. Vijayan, J. (2005) Data security risks missing from disaster recovery plans, *Computer World*, 39, 41, 16-18.

91. Weber, R. (1985) Basic content analysis, Sage, London.

92. Weiss, T. (2008) Gustav finds IT execs prepared for the worst, *Computer World*, 42, 32, 4.

93. Wild R., Griggs, K., Li, E. (2005) An architecture for distributed scenario building and evaluation, *Communications of the ACM*, 48, 11, 80-86.

94. Zalud, B. (2008) Continuity behind the lines, *Security*, 4, 2, 108.

APPENDIX A: CODING SCHEMES

Initial coding scheme, adopted from Fitzgerald and Dennis (2005):

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 B: 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
Chisholm, 2008
Connor, 2005a
Connor, 2005b
Cox, 2007
Crowe, 2007
Curtis, 2008
D'agostino, 2006
Davis, 2001
Defelice, 2008
Denyer, 2008
Dignan, 2004
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, H., Fisher, S., Thibodeau, P. (2006
Hayes, 2005
Hoge, 2005
Holliday, 2008
Hurdis, 2008
Jackson, 2008
Jaques, 2006
Jepson, 2008
Kepczyk, 2008
Kumar, et al., 2008
Laliberte, 2007
Landa, 2008
Lanter, 2008
Lindstedt, 2007
Lohrman, 2007
Lundequist, 2001
McAdams, 2008
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