Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, April 2010, vol. 15, no.1
(*http://www.arraydev.com/commerce/jibc/*)

Best Practices in IT Disaster Recovery Planning Among US Banks

Christopher Kadlec, PhD
First Author's Title/Affiliation: **Assistant Professor of Information Technology, Georgia Southern University, Statesboro, Georgia, United States**
Postal Address: **PO Box 8150 Georgia Southern University Statesboro GA, 30460**
Email: ***ckadlec@georgiasouthern.edu*** **(please use to correspond with the authors)**
Dr. Kadlec is an assistant professor or Information Technology at Georgia Southern University. His research interests include power-users, IT disaster recovery planning, and self-regulated learning.

Jordan Shropshire, PhD
Assistant Professor of Information Technology, Georgia Southern University, Statesboro, Georgia, United States
Postal Address: **PO Box 8150 Georgia Southern University Statesboro GA, 30460**
Email: ***jshropshire@georgiasouthern.edu***
Dr. Shropshire is an assistant professor of Information Technology at Georgia Southern University. His research interests include networking, security, IT disaster recovery, and IT in the banking and healthcare industries. He has published numerous articles in IS journals and conferences.

Abstract

In a recent study, it was found that as many as 60% of US enterprises don't have IT disaster recovery plans. The majority of IT disaster recovery planning guides are either inconsistent or so complicated that the average IT department can't commit the resources to completing them. In either case, the results are the same: the organization is not prepared to cope with IT-related disasters. This study reports on the IT DR planning practices of 154 banks in the United States. Surprisingly, neither IT budget nor IT department size were found to be common denominators among organizations with

adequate IT disaster recovery plans. The results of the study indicate that well-prepared firms perform some variation of the following seven activities: conduct IT service analysis, provide employee training, select methods of IT disaster identification and notification, define backup procedures, determine offsite storage locations, determine recovery procedures, and perform ongoing maintenance.

Keywords: **banking; information technology (ICT); Disaster recovery planning; research study; United States**

INTRODUCTION

Stable, reliable IT services have become the required minimum. Modern banks and financial institutions cannot function without information systems for data processing, storage, and communication (Rai and Mohan, 2006). At the same time, the list of risks to IT continually increases. Critical files may be lost or deleted. Hackers prey on susceptible web interfaces (Lallmahamood, 2007). Key employees may jump ship; they may become ill or incapacitated. Insiders may sabotage systems. Pandemics can temporarily wipe out entire organizations. Unexpected storms threaten physical infrastructure. In short, IT is both critical and vulnerable.

It is not possible to ignore risks to information technology. IT is such an integral part of banking operations that it has become necessary to conduct disaster recovery planning on an ongoing basis (Vijayan, 2005). This is underlined by the fact that federal agencies now specify IT disaster recovery planning guidelines which banks must follow (Plotnick, 1999). The purpose of such plans is to ensure the recovery of IT services following disaster (Gold, 2007; Sheth *et al.*, 2008).

IT disaster recovery planning is not an easy task. The complexity of modern information systems and the rapid pace at which technology change makes it very difficult to ensure that the proper steps are being taken (Retelle, 2008). Mainframes regularly process thousands of transactions. Internal applications are always being developed, modified, integrated, and retired. Desktop PCs must be maintained. Cut-throat competition allows customers to demand new services. Developing IT disaster recovery plans and getting them right is an increasingly difficult task.

In order to meet these objectives, a study was conducted in the summer of 2009. This included a mail-out survey to banks in the southeastern United States. The data collected from the survey was used to form the basis for this report.

This manuscript is organized as follows: The next section provides a general framework of IT disaster recovery planning. The following section describes the manner in which the data were collected and analyzed. The fourth section presents the results of the study, while the fifth section provides recommendations for improvement. The last section includes concluding comments from the authors.

BACKGROUND

Providing a single, holistic outline of an IT disaster recovery plan is a difficult task because organizations differ according to their information technology architectures and their delivery of IT services (Chun and Moody, 2009). Even among banks with relatively similar characteristics, there may be significant differences. However, it is possible to discuss the core steps which all organizations should follow when conducting IT disaster recovery planning. From a global perspective, IT disaster recovery planning is described as the set of actions which organizations follow in order to improve their ability to resume IT services following disaster (see Figure 1). Kadlec and Shropshire (2009) seven categories of actions:

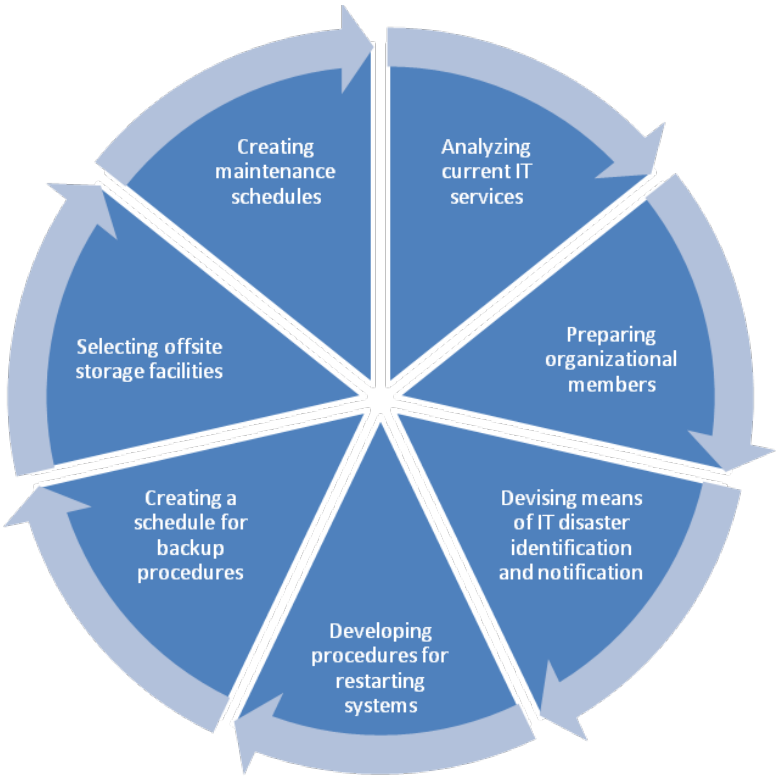

Figure 1: IT Disaster Recovery Plan Elements

Analyzing IT Services

Procedures for cataloging IT services, prioritizing IT services in terms of reactivation, and identifying potential threats. In total, there are three separate elements:

- IT Services Identification – comprehensive listing 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.

Preparing Organizational Members

Procedures for IT disaster recovery team training, briefing for key non-team members,

and the formalization of a decision-making structure. Specifically, there are three separate elements:

- Disaster Recovery Team Preparation - team assignments and responsibilities during the disaster.
- Non Team Preparation - training and briefing of non-team members in the event of a disaster.
- Decision Making - Formalization of a decision making structure.

Devising means of IT disaster identification and notification

Procedures for detecting IT disasters, for communicating during emergencies, and for warning IT disaster recovery team members and other stakeholders
In particular, there are three separate elements:

- 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.

Developing procedures for restarting IT services and systems

Procedures for restarting systems following disaster In particular, there are two separate elements:

- Recovery Procedures - 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.

Creating a schedule for backup procedures

Procedures for creating backup copies of data, software, configuration files, and IT disaster recovery plans

Selecting offsite storage facilities

Procedures for ensuring that systems, software and data are made as portable as possible and for ensuring that offsite locations have been selected for use as backup storage sites. Specifically, there are two separate elements:

- Portability - procedures for ensuring that systems, software, and data are as portable as possible.
- Offsite backup locations - locations to backup data, software, configuration files, the IT disaster recovery plans.

Creating maintenance schedules

Procedures for testing and updating the IT disaster recovery plan and its associated documentation and for ensuring that the plan fits within the scope of the business continuity plan. In total, there are three separate elements:

- Testing and Updating - procedures to ensure adequate testing and updating of the disaster recovery plan.
- Documentation - recording the configuration and changes to systems, hardware, and software.
- Synchronizing - procedures to ensure the IT disaster recovery plan is part of the

business continuity plan.

METHODOLOGY

In order to appreciate the current trends in IT disaster recovery planning activities among US banks and financial service institutions, a study was conducted in the summer of 2009. So that a benchmark analysis could be conducted, a mail-out survey was distributed to 332 institutions of a professional trade association for banks.

Surveys were mailed to CEOs and bank presidents used items adapted from Kadlec and Shropshire (2009) (see Appendix A for a listing of the questions). The questions were derived specifically for the purposes of this study. A cover letter explained the purpose of the survey and included directions for its completion. Among these directions was the request to have the individual in charge of information technology complete the survey. Along with the cover letter and the survey, a self-addressed, business return envelope was included for returning the survey.

Alternatively, a web-based version of the survey was also available. The cover letter provided the web address of the survey and included an authentication code for activating the survey. Later analysis indicated that there were no significant differences in responses between paper-based surveys and web-based surveys.

Some 156 surveys were returned, resulting in a 46.98% response rate. It may be assumed that nearly half of all banks in the state responded to this survey, resulting in a highly representative sample.

Once all the surveys were returned, the data was entered into spreadsheets for further analysis. Several statistical techniques were employed, including cross-tabulations and multivariate statistics. The findings of the analysis formed the basis of the results section.

RESULTS

The results of the analysis were organized so that a series of benchmarks could be established (see Table 1). As mentioned in previous sections, these benchmarks relate to IT disaster recovery planning activities, not parts of actual plans. They are grouped according to the seven categories of activities, and are summarized on the following table. The third column on the table indicates the percent of banks which perform each process.

Category	Elements	% Performing Activity
Analyzing IT services	IT Services Identification	68.4%
	Prioritizing IT Services	69.2%
	Risks to IT Services	73.7%
Preparing organizational members	Response Team Training	68.9%
	Personnel Briefing	63.7%
	Decision Making	73.2%

Devising means of IT disaster identification and notification	Detection	67.8%
	Warning	65.4%
	Means of Warning / Communication	74.6%
Developing procedures for restarting systems	Recovery Procedures	89.4%
	Alternative Facilities	83.1%
Creating a schedule for backup procedures		92.7%
Selecting offsite storage facilities	Portability	79.4%
	Offsite Backup Locations	83.8%
Creating maintenance schedules	Testing and Updating	88.7%
	Documentation	89.5%
	Synchronizing	87.3%

Table 1: Results of Study

Nearly all banks included in the study meet the IT disaster recovery planning guidelines specified by regulatory bodies (such as the FDIC and the FFIEC). In general, these requirements may be considered the core-technical elements of IT disaster recovery (see Figure 2). They include activities such as: creating backup copies of data and software, acquiring alternative technologies, and developing ways of resuming services.

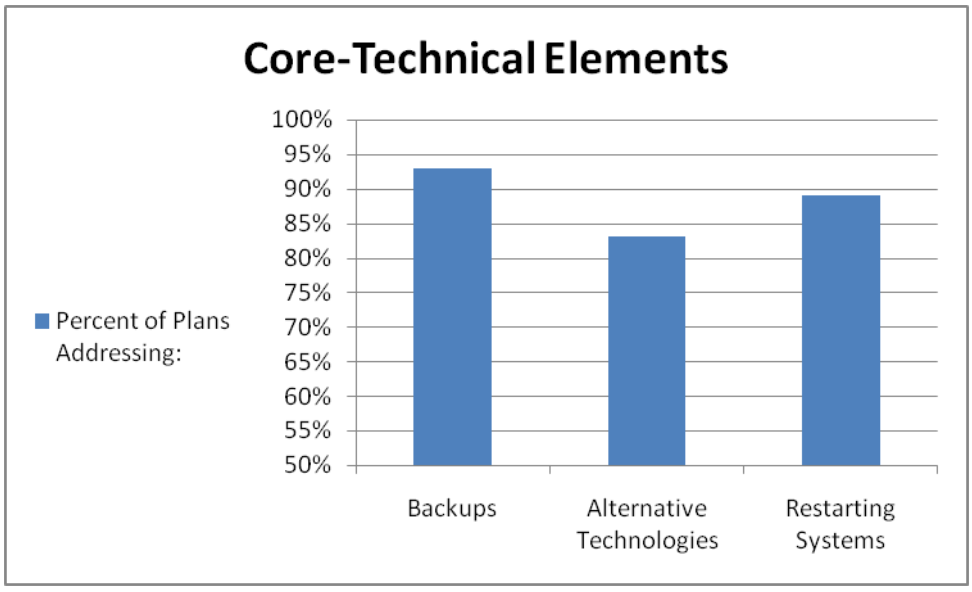

Figure 2: Core-Technical Elements

Beyond the core-technical elements, a number of other factors should be considered. These are the human elements of IT disaster recovery planning (see Figure 3). They include activities such as: creating IT disaster response teams, training personnel, warning employees of disasters, establishing communication channels, and formalizing decision-making authority. Within the sample, there is considerable variation in the degree to which these activities are performed.

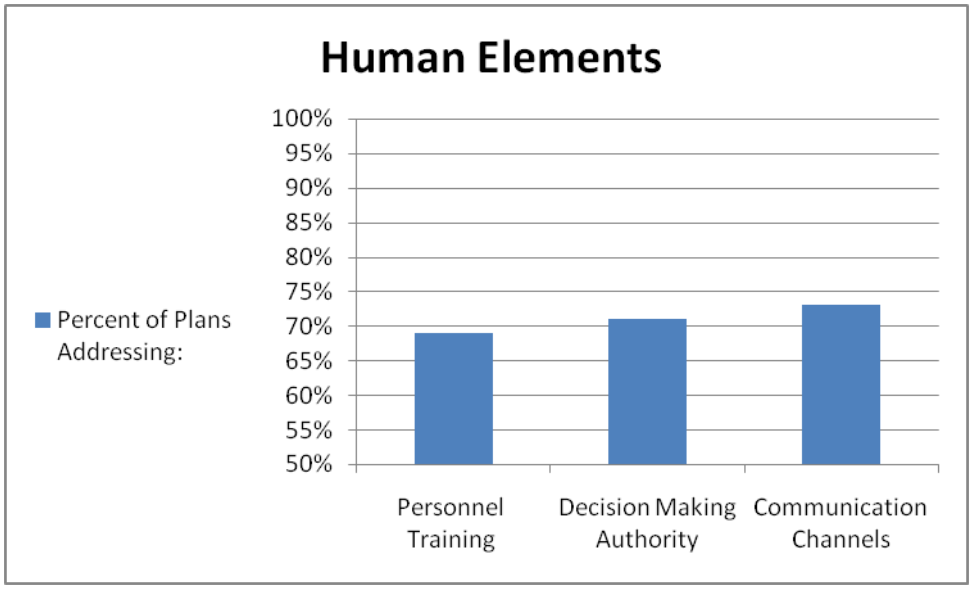

Figure 3: Human Elements

Further inquiries revealed that tech workers view IT disaster recovery planning as a technical exercise. They tend to discount the level of communication and coordination required to restore IT services.

RECOMMENDATIONS

The results of this study culminate in several key recommendations. Although they were based on the findings of banking organizations in the United States, they made be applied to other knowledge-based organizations which are subject to a high degree of regulation and publication oversight. Examples include the defense, healthcare, military, and airlines industries. The seven recommendations are:

IT Service Analysis

The top performers have a service mentality. They view their role as not just supporting information technology (routers and hard drives), but as providing information services (communications and record keeping). They know how their internal customers are using their offerings and they know which processes are dependent on certain systems. In cases of more than one IT service being lost, they have prioritized the order in which services should be reactivated. Each service is mapped to specific resources (software, hardware, data, and human expertise), and threats to each have been identified.

Employee Preparation

To capitalize on human resources and maximize efficiency, decision-making authority was formalized and IT disaster response teams were created. Well-prepared organizations ensure that not only are their teams up to date on training but key stakeholders are prepared for various scenarios.

IT Disaster Identification and Notification

The best organizations have guidelines for detecting IT disasters. They have established criteria for deciding which events may destabilize an IT service. This is especially important for IT shops with less experienced workers. In cases of disaster, they have procedures for activating the response team and warning key stakeholders. Because cellular towers occasionally fail and telephone lines may break, they have formalized an array of communication channels to be used in emergencies. Depending on the contingency, web-based message centers, calling trees or mobile phones may be used as backup.

Backup Procedures

Perhaps the most salient indicator of a well-prepared firm is the extent of its backup activities. Nearly all firms in the study backed up their data; most backed up their software. Few went on to save configuration files and still fewer had backup copies of their disaster recovery plans. Some firms elected not to create live backups (real-time replication of data in a secondary location), as it was found that identical copies of virus-infected databases are of little utility.

Offsite Storage

Because natural disasters can destroy physical computers and supporting infrastructure, the best-prepared firms used offsite locations for data storage and backup. This ranged from simply renting server space at a colocation facility to creating “hot sites” in different geographic areas. In addition, these firms ensured that their data, software, and configuration files were as portable as possible – that they were in a format amenable to transport to an alternative physical location.

Recovery Procedures

Surprisingly, many firms did not have actual plans for restarting services following disaster; they assumed that creating backup copies of data was sufficient. Those firms who had either previously experienced an IT disaster or had devoted considerable time to IT disaster recovery planning did have recovery procedures. Such plans accounted for a variety of contingencies, and, at a minimum, addressed each of the resources needed to provision IT services: physical facilities, human resources, communication technologies, servers, application systems, and data.

Maintenance

Well-prepared organizations viewed IT disaster recovery planning as an ongoing-process. They test and update their plans on a regular basis. Changes to IT services and their underlying resource inputs are noted and plans are updated. Finally, they ensure that the IT disaster recovery plan is synchronized with any business continuity plans.

LIMITATIONS

In a follow-up meeting related to this research, some of the IT leadership of some of the reporting banks suggested that there may be limitations to this research. It was suggested that some of the responses may be related to compliance to Federal

regulations. The basic concern was that if banks are compliant with regulations, they are not necessarily prepared for a disaster. Meeting Federal compliance does not mean that the ITDRP is sufficient to cover the complexity of an IT infrastructure in an individual bank. Additionally, being compliant on many distinct pieces of a plan does not mean that the plan will work. Lastly, it was pointed out to the researchers that if significant portions of the IT infrastructure for a bank are outsourced, the bank may believe that the ITDRP of the organization handling their IT infrastructure will be sufficient to cover the needs of the bank.

CONCLUSION

It is noted that IT disaster recovery planning work is not glamorous. It involves the painstaking creation of plans which may never be used (but must constantly be tested and updated). The value associated with this process is not immediately salient or easily quantifiable. Possible benefits would be derived from IT departments' better understanding of the business use of their systems, users' increased appreciation of their own reliance on technology, and organizations which are better prepared for change, be it initiated by disaster or opportunity. IT departments need to position themselves as being a mechanism for change and not a center for cost. In times of tightened budgets, convincing management to invest in IT disaster recovery planning can be a hard sell. However, the organization may already be performing most of the activities associated with ITDR planning. For instance, the organization may conduct an analysis of its IT services on a regular basis as a tool for ensuring the quality and usefulness of IT services. ITDR planners could make use of this analysis and save valuable time by skipping a step. Employee training can be costly; if the organization is already providing training for information systems usage, it might be possible to add content regarding IT disaster recovery and save money. In times of shrinking profits, it should be easier to sell the idea that ITDRP makes the organization more flexible and adaptable, and prepares employees to tap into new revenue streams.

REFERENCES

Chun M. and Moody, J. (2009) CIO roles and responsibilities: Twenty-five years of evolution and change. *Information & Management,* 46 (6), 323-334.

Gold, L. (2007) Disaster recovery planning: How do you measure up? *Accounting Today*, 21 (7), 31-35.

Kadlec, C. & Shropshire, J. (2009) Establishing the IT disaster recovery construct. *15th Americas Conference on Information Systems*, San Fransico, CA.

Lallmahamood, M. (2007) An examination of individual's perceived security and privacy of the internet in Malaysia and the influence of this on their intention to use e-commerce: Using an extension of the technology acceptance model. *Journal of Internet Banking and Commerce*, 13 (1).

Plotnick, N. (1999) When disaster plans fall short. *PC Week*, 28 (2), 58.

Rai, S. & Mohan, L. (2006) Business continuity model: A reality check for banks in India. *Journal of Internet Banking and Commerce*, 11 (2).

Retelle, M. (2008) Plan for disaster. *Credit Union Magazine*, 21(9), 80.

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.

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

Appendix A: Survey Instrument

Construct	Items	
Uncertainty Avoidance	UA1	It is important to have instructions spelled out in detail so that I always know what I'm expected to do.
	UA2	It is important to closely instructions and procedures.
	UA3	Rules/regulations are important because they inform me of what is expected of me.
	UA4	Standardized work procedures are helpful.
	UA5	Instructions for operations are important.
Long Term Orientation	LTO1	Careful management of money (thrift).
	LTO2	Going on resolutely in spite of opposition (persistence).
	LTO3	Personal steady and stability.
	LTO4	Long-term planning.
	LTO5	Giving up today's fun for success in the future.
	LTO6	Working hard for success in the future.
IT Disaster Identification and Notification Procedures	I1	We have procedures for detecting IT disasters
	I2	We have a means of assessing the magnitude of IT disasters
	I3	We have procedures for alerting individuals responsible for IT disaster recovery
	I4	We have procedures for letting stakeholders know that an IT disaster has occurred
	I5	We have established an alternative means of communications (i.e. cell phones) to use in emergencies
Preparing Organizational Members	P1	We have an IT disaster recovery team (i.e. group of employees who are responsible for restoring IT)
	P2	Those responsible for IT disaster recovery have been assigned specific tasks for restoring IT services
	P3	Employees and other stakeholders know what to expect during IT disasters
	P4	We have an explicit chain of command for dealing with IT disasters
IT Services Analysis	S1	We have identified all IT services which the IT department offers
	S2	We have identified all system resources required to provide IT services
	S3	We have assessed risks to IT services and infrastructure
	S4	We have ranked the order in which IT services would be repaired, if a disaster occurred
Recovery Process	R1	Should our primary site go offline, we have a secondary site
	R2	Should our primary site go offline, we have procedures for relocating IT operations
	R3	Our plans account for possible losses of human resources (i.e. missing or injured IT workers)
	R4	We have procedures for restoring physical facilities such as physical buildings, power, and cooling systems
	R5	We have procedures for recovering communications technologies such cellular phones, email, and VOIP
	R6	We have procedures for recovering servers
	R7	We have procedures for recovering applications and software
	R8	We have procedures for recovering data
Backup Procedures	B1	We have procedures for creating backup copies of data
	B2	We have procedures for creating backup copies of software
	B3	We have procedures for creating backup copies of configuration files, change logs, and other documents
	B4	We have procedures for creating backup copies of the disaster recovery plan itself
Offsite Storage	O1	We have ensured that system resources are as portable as possible (i.e. that they can be transported)
	O2	We have offsite locations for storing data
	O3	We have offsite locations for storing software
	O4	We have offsite locations for storing configuration files, change logs, and other relevant documents
	O5	We have offsite locations for storing copies of the IT disaster recovery plan
Maintenance	M1	We have procedures for testing of the IT disaster recovery plan
	M2	We have procedures for updating the IT disaster recovery plan
	M3	We have procedures for ensuring that the IT disaster recovery plan is part of the business continuity plan
	M4	We have procedures for documenting system configurations, changes, and updates