2000

A Contingency Model of IT Disaster Recovery Planning

Klara Nelson
Wayne State University, ad6425@wayne.edu

A Contingency Model of IT Disaster Recovery Planning

Klara Nelson, Department of Information Systems and Manufacturing,
Wayne State University, Detroit, ad6425@wayne.edu

Abstract

The dependence on information technology (IT) in all functional areas of the organization as illustrated during the recent Y2K crisis clearly demonstrates the need for effective IT contingency planning and disaster recovery strategies. To date, research on IT disaster recovery planning is very sparse. The present study aims at broadening our understanding of why some firms appear to be more crisis prepared than others and proposes a contingency model of IT disaster recovery planning. It extends previous research on IT planning by testing the utility of the strategic grid model for IT disaster planning.

Introduction

The great dependence of organizations on information technology (IT) as illustrated by the Year 2000 crisis necessitates effective IT contingency planning and disaster recovery strategies. The average business, for example, has its entire system shut down nine times per year. 50% of those firms whose critical business systems go down for 10 days or more never recover, and 93% of the companies with no recovery plan fail within five years (Louderback, 1995). The costs associated with system outages are considerable: computer downtime costs the USA $4 billion annually, and the average cost per four-hour outage is US $30,000. Despite its importance, empirical research on IT disaster planning is sparse. Prior research has focused on the phases of the planning process (Rohde and Haskett, 1990) and the disaster preparedness of small businesses with micro-computer based information systems (Vijayaraman and Ramakrishna, 1993). Drawing on the crisis management and IT planning literatures as well as on case studies of IT disasters, this research aims to broaden our understanding of why some firms appear to be more disaster prepared than others.

IT Disasters

Disaster in the context of computer and communication systems has been defined as an interruption of mission-critical information services for an unacceptable period of time(Toigo, 1996). This definition of disaster is akin to Weick's definition of a crisis as low probability/high consequence events that threaten a firm's most fundamental goals of survival and profitability (Weick, 1988). Crises usually occur when an environmental threat interacts with an internal weakness (Shrivastava and Mitroff, 1987). An extensive list of information systems disaster categories is provided by Vijayaraman and Ramkrishna (1993). Time is a multiplier of loss exposure (Toigo, 1996): the longer the company is without critical and vital business functions, the greater the costs of the outage and the less likely the possibility of full recovery. Maximum acceptable downtime and recovery window figures vary by industry, with financial companies having the lowest tolerance of interruption while manufacturing concerns, insurance companies, and other industries may survive for a longer period of time following an interruption (Toigo, 1996).

IT Disaster Management

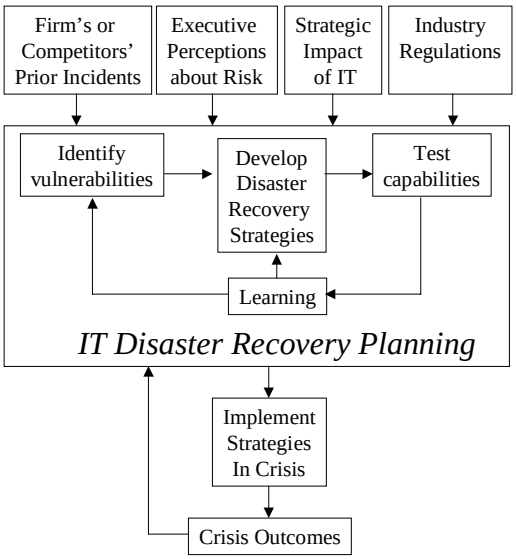
Defined as the process of examining the possibilities of losing an IT system and formulating procedures and strategies to minimize the damage (Haag, Cummings, and Dawkins, 1998), IT contingency planning begins with identifying the functions or business processes critical to a company's success and balancing the cost of unavailability with the cost of recovery. The purpose of effective disaster management is to ensure that "operations are sustained or resumed, organizational and external stakeholder losses are minimized, and learning occurs so that lessons are transferred to future incidents" (Pearson and Clair, 1998, p.60). Its effectiveness may be measured in non-events - disaster potentials that have been minimized or eliminated (Toigo, 1996). Disaster planning recovery strategies can be categorized according to the degree of confidence they provide: from high-confidence, expensive full redundancy options to low-confidence, low-cost laissez faire strategies. Regular testing of the plans is critical to uncover and fix major flaws before disaster strikes. Some companies such as John Wiley & Sons test their systems every six months (Hoffman, 1996) while others test their plans on an annual basis. Resource allocation in terms of funds and personnel vary, and cost and labor considerations have prompted many firms to outsource IT disaster recovery to leading vendors such as Comdisco, Sungard, or IBM (Dekleva, 1994; Hoffman, 1997).

A Contingency Model of IT Disaster Planning

Previous research in IT and crisis management suggests a contingency model of IT disaster planning behaviors. Figure 1 shows that the IT disaster recovery planning process (adapted from Kovoor-Misra, 1995) is influenced by the strategic role of IT, executive perceptions of risk and the usefulness of IT planning,

legal requirements, and prior exposure to accidents, incidents, or disasters by a firm or its competitors.

Figure 1. Contingency Model of IT Disaster Planning



Strategic Impact of IT

McFarlan, McKenney, and Pyburn (1983) argue that the development of an appropriate management strategy is contingent upon two factors: the strategic impact of existing systems to the organization's survival, and the strategic impact of the applications development portfolio. The congruency perspective suggests that the characteristics of an organization as determined by the strategic grid are associated with the type of information systems planning approach it adopts (Tukana and Weber, 1996). The strategic grid model has clear implications for IT contingency planning. If IS plays a strategic operational role, it must be insulated from the risks of any major operational disasters resulting in planning procedures for such contingencies (Raghunathan and Raghunathan 1990). This should also hold true for factory type organizations. In organizations where the development of future systems is important (turnaround and strategic organizations) procedures should be set up for regularly updating contingency plans to include the new technologies. Support organizations are expected to be least prepared for IT disasters.

Legal Requirements

Legal requirements are a major driving force behind disaster-preparedness in industries such as banking and insurance, where IT has played a predominantly strategic role (DiMartini, 1996; Toigo, 1996). For example, the Federal Financial Institutions Examination Council (FFIEC) stipulates inclusion of corporate-wide recovery planning in all banking operating areas and assurance that all banks maintain and exercise such plans. Regulations are not always observed, however. The Federal Deposit Insurance Corporation (FDIC) in 1992 for example ordered a small bank to obtain a computer hot site and develop a data processing business recovery plan within six months (DiMartini, 1996). However, in the absence of top management commitment to disaster planning, the effectiveness of such plans may be questionable (Pearson & Clair, 1998).

Executive Perceptions about Risk and Usefulness of Planning

IT disaster planning should be an integral component of corporate risk management. Previous research in crisis and strategic management suggests that top management support is a critical prerequisite for the development of crisis plans. When executives believe that their company is relatively immune to crisis and see little value in the usefulness of contingency planning - the "it-won't-happen-to-us" syndrome that is not uncommon in large companies -, preparation will be less likely in place to contain or prevent a crisis. Even where crisis preparations are regulated, executive perceptions must support crisis management programs to be highly effective (Pearson & Clair, 1998). Following Dutton (1986), one can argue that the more an issue is perceived to be a crisis prone issue, the greater the resources devoted to resolve the issue.

Prior Incidents

A final driving force behind contingency planning is the occurrence of prior incidents in the company or one experienced by a competitor (Edwards and Reising, 1996).

Hypotheses

Based on the previous discussion, the following hypotheses will be tested:

1) The *strategic impact of existing systems* is related to its disaster planning strategies.
   a) *Resources provided for IT disaster planning*: The greater the impact of existing systems to the firm's survival, the greater the amount of resources devoted to IT disaster planning.
   b) *Type of disaster recovery strategies*: The greater the impact of existing systems to the firm's survival, the greater the use of high-confidence strategies in IT disaster planning.
   c) *Testing of strategies:* The greater the impact of existing IT on the firm's survival, the greater the likelihood that plans are regularly tested.
2) The *strategic impact of the applications development portfolio* is positively related to extent to which *plans are regularly updated.*

3) *Perceived usefulness* of IT disaster planning will be highest in organizations where the strategic impact of both existing and future applications is high, and lowest in organizations where the strategic impact of both existing and future systems is low.
4) *Executive perceptions about risk* are positively related to the degree of crisis preparedness. The higher the degree of perceived risk, the greater the degree of crisis preparedness.
5) The greater the number of *prior incidents* experienced by the firm or its competitors, the greater the extent of crisis preparations.
6) *Industry regulations* are positively related to the extent of IT disaster planning.

Research Methodology

Data will be collected via a mail survey from top IS executives in a wide range of randomly selected industries obtained from the most recent edition of the *Directory of Top Computer Executives*. These executives are assumed to be in the best position to have a holistic view of all IS functions, including disaster recovery. A questionnaire has been developed and pilot tested. Part I of the questionnaire collects background information. Part II assesses the company's overall IT strategy, dependence on existing information systems for line and staff/administrative support functions, financial impact of IS interruptions, and maximum acceptable downtime. Items in Part III address the strategic impact of the applications portfolio under development. Questions in Part IV concern the disaster preparedness of a firm in terms of the existence of a formal disaster recovery plan, perceptions about the usefulness of such a plan, resources devoted to IT disaster recovery planning, perceptions about risk associated with a variety of threats, occurrence of such threats, backup strategies, recovery strategies for data centers and networks, and testing and updating of a disaster recovery plan. Data collection has begun and preliminary results should be available at the AMCIS 2000 conference in August.

References

Dekleva, S. M. "CFOs, CIOs, and Outsourcing," *Computerworld*, May 16, (28:20), 1994, p. 96.

DiMartini, W. P. "What Drives Contingency Planning - The Carrot or the Stick?," *Contingency Planing & Management*, March 1996, pp. 15-19.

Dutton, J. E. "The Processing of Crisis and Non-Crisis Strategic Issues," *Journal of Management Studies*, (23:5), 1986, pp. 501-517.

Edwards, S. and Reising, J. "Fortune 1000 Companies Commit to Crisis Management," *Contingency Planing & Management*, May 1996, pp. 9-11.

Haag, S., Cummings, M. and Dawkins, J. *Management Information Systems for the Information Age*. Boston, MA: McGraw Hill, 1998.

Hoffman, T. "Publisher does Disaster Planning by the Book," *Computerworld*, May 20, (30:21), 1996, p. 74.

Hoffman, T. "Labor Drought spurs Flood of Disaster Outsourcing," *Computerworld*, August 4, (31:31), 1997, pp. 41-42.

Louderback, J. "Will You be Ready When Disaster Strikes?," *PC Week*, February 6, (12:5), 1995, p. 130.

McFarlan, F. W., McKenney, J.L. and Pyburn, P (1983). "The Information Archipelago - Plotting a Course," *Harvard Business Review*, January-February, 1983, pp. 145-156.

Kovoor-Misra, S. "A Multidimensional Approach to Crisis Preparation for Technical Organizations: Some Critical Factors," *Technological Forecasting and Social Change*, 48, 1995, 143-160.

Pearson, C. M. and Clair, J. A. "Reframing Crisis Management," *Academy of Management Review*, (23:1), 1998, pp. 59-76.

Raghunathan, B. and Raghunathan, T. S. "Planning Implications of the Information Systems Strategic Grid: An Empirical Investigation," *Decision Sciences*, (21:2), 1990, pp. 287-300.

Rohde, R. and Haskett, J. "Disaster Recovery Planning for Academic Computing Centers," *Communications of the ACM*, (33:4), 1990, pp. 652-657.

Shrivastava, P. and Mitroff, I. "Strategic Management of Corporate Crises," *Columbia Journal of World Business*, (22:1), 1987, pp. 5-11.

Toigo, J. *Disaster Recovery Planning for Computers and Communication resources*. New York: John Wiley & Sons, Inc., 1996.

Tukana, S. and Weber, R. "An Empirical Test of the Srategic-Grid Model of Information Systems Planning," *Decision Sciences*, (27:4), 1996, pp. 735-765.

Vijayaraman, B. S. and Ramakrishna, H. V. "Disaster Preparedness of Small Businesses with Micro-Computer Based Information Systems," *Journal of Systems Management*, (44:6), 1993, pp. 28-32.

Weick, K. E. "Enacted Sensemaking in Crisis Situations," *Journal of Management Studies*, 25, 1988, pp. 305-331.