Disaster Recovery Planning for Information Systems

SOOUN LEE
Miami University (Oxford, Ohio)

SCOTT ROSS
Information Systems Analysis at GIS of AT&T

In a society where individuals are linked to one another through the conduits of expansive technology, nearly everyone has experienced, or at least witnessed, the vast devastation which occurs when disaster strikes. The need for businesses to have the ability to survive when any form of disaster strikes becomes paramount as more and more US corporations are relying on data and information systems (IS) for performing their main operations. Authors are suggesting a five-step guideline for developing and implementing a disaster recovery plan (DRP).

In a society where individuals are linked to one another through the conduits of expansive technology, nearly everyone has experienced, or at least witnessed, the vast devastation which occurs when disaster strikes. The need for businesses to have the ability to survive when any form of disaster strikes becomes paramount as more and more US corporations are relying on data and information systems (IS) for performing their main operations. Authors are suggesting a five-step guideline for developing and implementing a disaster recovery plan (DRP).

The types of disasters which affect operations of information systems within organizations can be divided into three basic categories (Bohacek, 1990):

- Natural disasters - (i.e., earthquakes, fires, floods, hurricanes, and tornadoes)
- Inadvertent errors - (i.e., problems with software)
- Deliberate actions - (i.e., viruses and worms.)

Even though the need for organizations to develop effective strategies for a DRP stems mainly from an awareness of how a major disaster can affect business, what must be recognized is that it is often the more mundane problems (the accidental triggering of a fire sprinkler over the computer information systems equipment) which are most apt to bring business to a halt (Clifford, 1990). Recently, federal legislation requires some companies to develop and test disaster plans. National banks must comply with the 1983 Banking Circular 177, which states that a bank must develop means to...
reduce the impact and/or risk of losing data processing (DP) support (Wong, et al., 1994). The companies that electronically transfer funds in excess of $20 billion per day must show the ability to recover from a disaster within 24 hours (Wong, et al., 1994).

This need for business to have the ability to survive when any form of disaster strikes becomes even more paramount when recognizing that the majority of the American work force is critically dependent upon receiving, modifying, generating, and distributing information (Bohacek, 1990). An estimated 60 percent of the US work force consists of individuals whose jobs are “critically dependent” upon information (Bohacek, 1990). As the role of information systems becomes even more pervasive amidst the transition to an information-based society, the need for organizations to be fully prepared when disaster strikes becomes critical. The reality of the current situation dictates that businesses become proactive in developing solutions for restoring information systems in the event of disaster because, simply put, a reactive method will not meet the needs of an organization’s customers and business will grind to a halt. Although it is inevitable that disasters will occur, what must be recognized is that the damaging effects of such incidences can be mitigated by strategically developing and implementing a DRP (Bohacek, 1990).

There are many issues which merit consideration when an organization is creating a DRP. Authors are suggesting the following five-step model (See Figure 1) to provide a guideline for industry practitioners when they construct a DRP to meet their business’ needs.

**Justification**

According to Jack Bannan, manager of information security for General Electric and cofounder and president of the Delaware Valley Disaster Recovery Information Exchange, the real problem in the corporate environment is that in most organizations, disaster avoidance is such an exceedingly obvious issue that it is everyone’s responsibility, and yet no one is really in charge (Rothstein, 1988). As Bannan points out, “Very few board chairmen, presidents, or general managers would run a business without insurance. For some reason, they have yet to look at DRP in that same light” (Rothstein, 1988). This is somewhat paradoxical in the sense that most businesses are now heavily reliant upon some form of computer information systems in their everyday operations, yet very few have taken measures to prepare for when disaster strikes. In fact, it is estimated (Clifford, 1990) that a mere 15 to 20 percent of US corporations have DRPs (some organizations prefer to refer to such plans as “business contingency proposals”). Of the small number of corporations that do have such plans, fewer than 25 percent have ever tested their plans to see if they would perform adequately should the need arise.

Clearly, there seems to be something which is standing in the way of businesses incorporating such plans as a feature of the organization’s operations. Perhaps the greatest barrier to widespread development of DRPs in corporate America today is the cost associated with the development and implementation of such strategies (Falconer, 1990).

It is the tradition that computer information systems operations have not been designed to provide continuity in the event of a disaster simply because the associated cost has been deemed too great. Recovery planning, not unlike term insurance, has no immediate return on investment (Clifford, 1990). This element together with the current economic uncertainty makes it very difficult for most businesses to justify the expenditure which is necessary to incorporate an effective contingency plan. Therefore, in many organizations, the greatest obstacle which must be overcome is adequately justifying the cost associated with planning in order to draw an approval and/or commitment from the top management.

Acting as yet another impediment which corporations must deal with when coordinating a disaster recovery approach is the difficulty they face when attempting to accurately quantify the potential financial impact a disaster could have upon their organization (Clifford, 1990). Xephon, the UK-based IBM analysts, published a survey of disasters in its IBEX Bulletin, covering experiences, at over 800 cites worldwide; 22% of sites had experienced a disaster of some sort. The average cost of a disaster worked out at $32,000; with power failures averaging over $110,000 and fires over $60,000 (Norman, 1993). It is rather simple to compute hourly, daily or even monthly losses based on previous records of an organization’s transactions. What must be recognized, however, is that the costs which are incurred when an organization is affected by a disaster, no matter what kind, extend well beyond the mere scope of dollars lost. It is imperative that businesses also consider the rather “intangible” costs that are also associated with such events. These rather elusive conse-

---

**Figure 1. Five Step DRP Model**

- **Step 1: Justification of the plan**
- **Step 2: Inventory Determination**
- **Step 3: Disaster Recovery Strategy**
- **Step 4: Personnel Assignment and Training**
- **Step 5: Test and Maintenance**
4 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:
www.igi-global.com/article/disaster-recovery-planning-information-systems/51011?camid=4v1

This title is available in InfoSci-Journals. Recommend this product to your librarian:
www.igi-global.com/e-resources/library-recommendation/?id=2

Related Content

Demonstrating Value-Added Utilization of Existing Databases for Organizational Decision-Support
www.igi-global.com/article/demonstrating-value-added-utilization-existing/1227?camid=4v1a

Network Effects of Knowledge Diffusion in Network Economy
www.igi-global.com/chapter/network-effects-knowledge-diffusion-network/13981?camid=4v1a

Remote Management of a Province-Wide Youth Employment Program Using Internet Technologies
Bruce Dienes and Michael Gurstein (1999). Success and Pitfalls of Information Technology Management (pp. 159-173).
www.igi-global.com/chapter/remote-management-province-wide-youth/33489?camid=4v1a

Critical Chain Method in Traditional Project and Portfolio Management Situations
www.igi-global.com/article/critical-chain-method-in-traditional-project-and-portfolio-management-situations/119531?camid=4v1a