SCOTTSDALE INSTITUTE

INFORMATION EDGE

A CEO Resource for Managing Clinical Information Systems

January 1999
Volume 5, Number 1

Disaster Recovery Planning for Enterprise-wide Computing

Jim Edgemon and Mark Lemak, First Consulting Group

Executive Summary

As healthcare organizations depend increasingly on information technology to support patient care and business operations, a solid disaster recovery plan has become a strategic imperative. The loss of the computer network or clinical and business applications, even for a short period of time, can have serious financial, patient care, and regulatory repercussions. At best, failure by healthcare management and clinical leadership to plan for disaster recovery may violate JCAHO regulations. At worst, it may hinder critical patient care processes. Consider the following examples:

- Physicians depend on the Laboratory Information System (LIS) to order tests and receive results. When a network or computer outage occurs and the LIS is unavailable, orders and results must be manually delivered between the Laboratory and nursing units. This manual process slows the Lab's ability to process requests and results; consequently, patient care suffers.

- The Radiology Department depends on the Radiology Information System (RIS) to provide patient histories, film location and tracking. When a network or computer outage occurs and the RIS is unavailable, technicians and medical staff do not have online access to images. Film room staff must search the extensive film archive manually to match patient names to the archived film jackets. This slows Radiology service levels to a crawl.

- The Operating Room (OR) depends on the Patient Scheduling System (PSS) to schedule surgeries, list physician preferences, and patient charge items. When the PSS is unavailable due to a network outage, the OR must manually add new surgeries to the last schedule printout.

- Hospital Call Centers providing medical treatment recommendations, poison intervention, or other emergency treatment recommendations are especially vulnerable to downtime and computer outages. In life and death situations when minutes count, downtime procedures may not provide the level of information required for split-second patient treatment decisions.

SCOTTSDALE INSTITUTE
MEMBERSHIP SERVICES OFFICE
1660 SOUTH HIGHWAY 100
SUITE 140
MINNEAPOLIS, MN 55416
(612) 545-5880
FAX (612) 545-6116
EMAIL scottsdale@fcgnet.com

Network outages and IT disasters create financial and patient care implications as well as legal and regulatory considerations for healthcare organizations. Increasingly, healthcare leaders are automating clinical processes to enhance performance and efficiency. As this trend continues and automation becomes entrenched in the clinical setting, the risk of a significant loss grows. Healthcare leadership could be held accountable by legal or credentialing organizations for a lack of disaster recovery planning:

The loss of the computer network or clinical and business applications, even for a short period of time, can have serious financial, patient care, and regulatory repercussions.

- The 1977 Foreign Corrupt Practices Act considers computer applications and corporate data critical assets. Extended network downtime that prohibits access to core financial and record-keeping applications could result in healthcare administrators being held individually liable in a court of law.

- Healthcare organizations, like private and publicly traded corporations, could be required in a court of common law to exercise "good business judgement." Since downtime can be avoided with proper planning and redundancy, the lack of a redundant network, disaster recovery plan, and/or appropriate downtime procedures may show failure to exercise "good business judgement."

- The Information Management section of the JCAHO standards manual states that healthcare organizations must be able to protect records and information against loss, destruction, tampering, and unauthorized access or use. To accomplish this objective, healthcare organizations must have a formal disaster recovery plan and some level of network redundancy.

Healthcare leadership could be held accountable by legal or credentialing organizations for a lack of disaster recovery planning.

Many healthcare organizations have a variety of computing platforms, including mainframes, midrange, minis, micros, and Local Area Networks (LANs). IT management should establish a planning process for all hardware platforms within the enterprise-wide network, providing for the resumption of enterprise-wide computing after a disaster. The recovery plan should include provisions for each location of the enterprise-wide network, so the resources required to quickly recover from a computing outage can be mobilized.

This report presents the fundamentals of comprehensive disaster recovery planning for an enterprise-wide computing environment, providing an overview of each component:

- Project kickoff
- Recovery requirements
- Recovery resources
- Recovery options
- Selecting recovery options
- Coping strategies
- Cost analysis

- Gaining approval
- Plan development
- Testing
- Plan maintenance

▲

Project Kickoff

Evaluating disaster recovery options for an enterprise-wide computing environment requires a formally organized project with the support of senior management and clinical leadership. The disaster recovery planning (DRP) project team should consist of representatives from computer operations, network operations, technical support, application programming, and clinical and business operating units. The project team must develop a work program that identifies specific areas to be covered, as well as a structure and approach for accomplishing major tasks and activities.

Evaluating disaster recovery options for an enterprise-wide computing environment requires a formally organized project with the support of senior management and clinical leadership.

Recovery Requirements

The DRP team must interview each operating unit to determine the impact an extended outage will have on operations. The team must document clinical and business functions served by each application, along with the necessary interfaces from other applications. They must evaluate possible coping strategies that would allow each unit to maintain critical clinical and business functions during a major network outage. Next, the DRP team should determine the costs required to maintain clinical and business functions during an enterprise-wide recovery. The DRP team must also determine the desired time frames for recovery of automated support. When the interviews are completed, the DRP team evaluates recovery strategies for each application according to its hardware platform.

Recovery Resources

The DRP team must identify, inventory, and document all hardware computing platforms, hardware components, systems, support software, and operations software at each location of the enterprise-wide network. They must also document existing facilities and environmental requirements for each location. They should conduct departmental surveys at each major location, including questions on resource usage, user-processing schedules, and technical/data resources (e.g., computer hardware, software, data files, data communications, and application programs) needed by each application. In addition, the DRP team must identify the size of these items required for a complete recovery of enterprise-wide operations. Disk Space is a particularly critical resource due to the cost and time required to acquire, install and relocate data files.

The DRP team must interview each operating unit to determine the impact an extended outage will have on operations.

Recovery Options

The DRP team must examine available recovery options for all enterprise-wide applications, evaluating each major option based on the healthcare

organization's ability to deliver patient care during recovery. Recovery options include strategies that can serve as alternatives for contingency planning, ranging from simple to complex. Some of these alternatives could represent a complete plan; more likely, a combination of alternatives will be required.

Deferment of Processing – This option assumes that applications are not needed immediately after a disruption occurs. The user departments would prepare, organize, and log source documents for data entry or document scanning while enterprise-wide recovery was in process. Using an outside data entry service could speed the data preparation.

Clerical Maintenance – Given certain assumptions, this process might be used to maintain critical patient care functions during the recovery period. The clinical and business units would need to have the necessary staffing and facilities available. Also, the department would need to obtain files from off-site storage and supplies from local or remote vendors. The daily operating procedures for the clinical and business units would need to be revised to accommodate the loss of automated information support. These emergency procedures must plan for staffing and facilities to accommodate peak workloads.

Off-the-shelf Equipment – This option affords a practical recovery method if applications are processed on a distributed or stand-alone basis using microcomputers. Microcomputers can be purchased more quickly than their mainframe counterparts, and they have minimal environmental requirements. If the DRP team chooses this strategy, they must establish contracts with capable vendors and specify the delivery timeframes necessary to support recovery operations.

Warehousing Equipment – Warehousing equipment must be considered when computer hardware and related equipment require longer lead times than the off-the-shelf strategy. Using this recovery approach, the DRP ensures additional computer hardware is maintained off-site for recovery purposes. The off-site computer hardware must be under maintenance agreement with a vendor who will relocate the equipment if a disaster occurs. The DRP team must test the off-site computer hardware regularly as part of their disaster recovery plan.

Reciprocal Agreements – Reciprocal agreements are formal agreements between two entities to provide recovery backup for each other if a disaster occurs at either site. Hardware compatibility is an ongoing concern with this type of agreement. The agreement must clearly define the critical applications, processing resources, schedules, and staffing required in the event of a disaster. Both sites must conduct regular recovery testing to ensure software compatibility. Should either company declare a disaster, both companies must be willing to operate in a disaster mode.

Service Bureaus – This plan handles specific processing requirements during in-house recovery efforts. It may extend in-house recovery time frames and provide the healthcare organization with greater recovery flexibility. This approach is useful for stand-alone applications that do not have on-line interface requirements. The DRP team will need to negotiate a formal contract and pay a retainer to ensure processing availability with the service bureau.

Multiple Data Centers – This option provides an extra degree of protection for the healthcare organization whose business requires high on-line availability. The organization distributes its normal workload between two remote data centers. Both data centers have the available capacity to handle the other's critical clinical and business functions. Should a disaster occur at the one site, each data center is prepared to operate all critical functions. Each site maintains close coordination to ensure compatibility with the other.

Third-Party (Hot Site) – Third-party services are provided by many vendors across the country. Hot site services are competitive; therefore, most companies go through a formal procurement process to get the best price, terms, and conditions. The hot site vendor charges a fee for subscribers. Should the subscriber declare a disaster, it can use the vendor's fully equipped hot site facility. While the subscriber is using the facility, the provider charges a daily usage fee. Usually, the subscriber is entitled to test its disaster recovery plan at the hot site twice each year. Hot site providers can also provide additional operational services under contract.

Hot site services are competitive; therefore, most companies go through a formal procurement process to get the best price, terms, and conditions.

If an organization develops a hot site recovery plan, it must include a strategy for transporting staff, tapes, and materials during an actual disaster. Generally, testing can be accomplished remotely. The recovery plan must include a data communications strategy to access company data from the hot site.

Company-Owned Cold Site – A company-owned, vacant computer facility equipped with all the environmentals required to receive and support the company's computer hardware. This includes the ability to re-terminate the hub of the company's data communications network from the cold site facility. If a company-owned cold site is a viable recovery option, IT management must acquire and install the necessary computer hardware in time to meet the company's recovery time frames for critical clinical functions.

Cold Shell Cooperatives – This option is similar to the third-party service: a subscription fee and contract entitles the company to access the cold site. This recovery approach is a good option when recovery times are less important. The company is responsible for equipment delivery, installation, and facility operations.

Selecting Recovery Options

The DRP team must evaluate recovery options for each location based on the application recovery requirements and hardware platform.

Mainframe – Recovery alternatives are based on how quickly critical applications must become operational after a computing outage. Companies in the banking, insurance and airline industries may have multiple data centers that can shift processing loads to back up other company sites during a major computing outage. Hot Site recovery approaches are effective when critical clinical and business functions can be maintained without mainframe support for at least forty-eight hours. This allows time to recover mainframe support from a company-owned or third party hot site.

Clinical and business units dependent on enterprise-wide computing must develop, document, and test procedures that provide critical functions during an enterprise-wide recovery.

If IT management can employ coping strategies to maintain critical clinical functions longer than forty-eight hours, a company-owned or third party cold site may be cost effective. Computer hardware must be delivered, installed, and accepted before recovery efforts can begin. Under normal conditions, it may take three to six weeks to have computer hardware purchased and delivered before recovery efforts can begin.

Midrange – System users have the same recovery alternatives available as their mainframe counterparts. Many companies have multiple midrange processors to spread their processing load and provide in-house recovery backup. Third-party hot site and cold site agreements are available with many third-party vendors. Many midrange hardware platforms do not require special facilities or special environmental conditioning to support their operations. Emergency midrange system operations could be established under normal office conditions. Some lower-end midrange systems could simply be warehoused for emergency deployment.

PC/LAN – Recovery alternatives for PC/LAN include equipment warehousing and an off-the-shelf approach. Some hardware vendors offer special arrangements to ensure equipment availability. Backup and recovery of critical LAN files may be challenging if a formal tape backup strategy is not employed. Some companies are backing up LANs on mainframes using special LAN backup and recovery software. This approach can provide recovery of a single LAN or the entire LAN environment. Should an area disaster occur, this approach would allow the organization to recover the entire LAN environment from a hot site after accomplishing mainframe recovery.

Coping Strategies

Coping strategies allow user departments to continue supporting critical clinical and business processes after a disruption of enterprise-wide computing. Clinical and business units dependent on enterprise-wide computing must develop, document, and test procedures that provide critical functions during an enterprise-wide recovery. Hot site coping strategies must provide for the maintenance of critical clinical and

business functions during the forty-eight hour recovery period when mainframe operations are being restored from the hot site. Cold site coping strategies must maintain critical clinical and business functions for a longer recovery period, which is based on the amount of time required for computer hardware replacement at the cold site. Coping strategy techniques include deferment of processing, clerical maintenance and microcomputer support.

Cost Analysis

The cost analysis for selecting the most cost-effective recovery option must include one-time implementation costs and first-year recurring costs. One-time costs include strategy development and site preparation. Recurring annual costs include testing, travel expenses, telecommunications, vendor subscription fees, and coping strategy maintenance. Insurance policies are available to financially support enterprise-wide recovery. Should a disaster occur, insurance policies will pay the hot site vendor's disaster declaration fee plus the daily usage fee. In addition, the policy will pay transportation and lodging expenses for employees, and transportation costs for delivering tapes to and from the hot site. These policies also cover employee overtime, data recreation, and computer hardware replacement.

Gaining Approval

The results and recommendations of the enterprise-wide disaster recovery-planning project must be packaged into a report for senior management and clinical leadership. The report should include an executive summary with bottom-line recommendations and a cost benefit analysis requesting management approval. The report must present a review of the tangible and intangible benefits covering the project approach, objectives, assumptions, disaster impact, resource requirements and recovery options. Attachments may provide details on each option and a summary of the activities required to support the project's recommendations.

Plan Development

After the recommendation is approved and the DRP team has selected the recovery approach for each node on the enterprise-wide network, their work is just beginning. The DRP team must conduct a series of structured workshops to develop the recovery scripts to be used during the actual testing. The recovery scripts must include sections clearly defining the activities of computer operations, technical support and applications programming during the recovery tests. The plan development is an iterative process that will be refined and improved as the team conducts tests and analyzes results.

Testing

Periodic testing is a crucial part of completing and maintaining the disaster recovery function. This testing must include enterprise-wide facilities, recovery procedures, and the recovery teams. IT management

must plan to test application systems regularly until all applications have gained a good recovery posture. Network contingency planning is just as critical as planning for computer and computer component recovery. Real-time transaction processing heightens the importance of data communication.

Plan Maintenance

The disaster recovery plan can never be considered complete. Ongoing disaster recovery plan maintenance is vital to ensure continued information systems capabilities. The expense of plan maintenance must be considered a "cost of doing business." A current and effective disaster recovery plan assures continued protection of the health care organization and its patients.

The disaster recovery plan can never be considered complete. Ongoing disaster recovery plan maintenance is vital to ensure continued information systems capabilities.

The Disaster Recovery Plan must be reviewed at least annually to certify its viability in response to changes in hardware, software, data communications, and clinical and business operations. Internal audit or a knowledgeable consulting firm should review the plan and recommend actions to ensure the plan remains current.

Conclusions and Recommendations

Developing a comprehensive recovery posture for an enterprise-wide computing environment is well worth the investment in time and money. As a first step, the IT department must gain management and clinical support approval to organize a disaster recovery planning project.

The DRP team must interview key staff in clinical and business operating units, documenting the recovery requirements for each application. How long can user departments maintain critical clinical and business functions without enterprise-wide computing operations? After the DRP team summarizes interviews and charts results into recovery time frames, they must identify recovery resources in terms of processing requirements, disk storage, tape storage, print volumes and connect hours. The team's next step is to compare all recovery resources, options, and time frames for each application. Comparing this research will allow the DRP team to see which option provides the best service level at the best price.

With these findings, the team should then develop a formal financial analysis identifying one-time costs and recurring annual costs for each major recovery option. Some disruption insurance policies will pay the disaster declaration fee, daily usage fee, transportation costs, lodging, overtime, data recreation and computer hardware replacement. Insurance policies can help improve the bottom-line cost for a hot site recovery over the cold site approach. As a precaution, the DRP team should perform a dry run of the final recommendation for internal or external auditors. Finally, the team should present recommendations to senior management and clinical leadership based on reduced risk, price performance, and level of service during recovery.

The healthcare organization's enterprise-wide recovery plan must undergo regular testing. Many organizations conduct two tests each year. The recovery team must have clearly defined duties that are scripted out in advance. The test plans should include goals and objectives for each test. A recovery coordinator must coordinate all test activities and document the results of each test. As changes occur in a healthcare organization's enterprise-wide hardware and software configuration, the DRP team should maintain and update the recovery plan. Since a solid disaster recovery plan requires frequent testing and reevaluation, it should be reviewed periodically by both internal audit and outside consultants. A necessity for any organization relying heavily on information systems, disaster recovery planning and maintenance should be a priority – not an option.

SI's Recommendations

1. The goal of disaster recovery is to eliminate single points of failure. The data center is just one of those points; the recovery plan should include the entire infrastructure. For example, instead of having all terminals in the ER connected to one control unit, split them up. If a single control unit fails, half the terminals will continue to operate. Establish two telephone links between a hospital and a data center in case one fails.

2. Not every application is a candidate for a hot site. A cost-benefit study may identify, for example, that a hot site is an absolute must for receivables but not for payables, or for a laboratory but not for order-entry.

3. Successful disaster recovery plans will involve testing recovery systems at least every quarter.

4. In addition to assigning a team to run the hot site, an organization should assign a second team to put the problem area back together.

5. Reciprocal agreements—where two hospitals agree to back up each other's systems in case of failure—look better on paper than in real life. Most reciprocal agreements are quite limiting because every time an organization modifies its systems, it must correlate the change with its partner.

▲

It should be on your desk!

Yes, the registration materials for our

Annual Membership Conference
April 7-9, 1999

have been mailed out to everyone.
Send your registration in today!

For further information, call the
SI Membership Services Office at 612/545-5880.