

Disaster Recovery Planning

Assess, Adjust, Improve

An LXI Publication

Your company's ability to recover is a high priority. In a survey by *Contingency Planning & Management Magazine* of 1437 contingency planners, 76% indicated that their organizations had reviewed their recovery/continuity plans, 10% have completely overhauled their plans, and 52% have made some changes since September 11. The question has changed from "can we recover?" to "how fast can we recover?"

A good Disaster Recovery plan is an essential step to recovery. This white paper combines LXI's expertise in technology and services to offer you ways to assess, adjust and improve your company's Disaster Recovery plan.

Expectations regarding data availability have changed. There are many terms used to describe a company's overall data protection strategy: high availability, business resumption and business continuity. Often these terms are used interchangeably when in fact; each one represents a completely different set of concepts, procedures, and principles.

It is important to clarify the differences so that everyone's expectations are based on the same general assumptions regarding the deliverables of each type of plan.

A Disaster Recovery plan lays out the procedures, steps, people, places, equipment, and priorities necessary to restore damaged or destroyed computer systems, as well as the peripheral infrastructure to resume business operations after an outage.

High availability uses technology, such as hardware devices or software products, to provide a continuous copy/replication of production data from a primary system/location to a secondary systems/location. A high availability solution provides 24/7 access to production data. This allows users to be switched to a secondary system when the primary system is down. Like the high availability solution, backup solutions also utilize software and hardware technologies to provide the quickest recovery for the entire system.

Business resumption plans assess and define how quickly specific applications have to be available to the users — some immediately; others based on business priorities and resources.

Applications such as order processing, customer service, and accounts receivable may have a higher priority, for example, than accounts payable.

It all comes down to business continuity. The software and hardware strategies needed to meet your business needs are discussed in detail throughout this white paper, including the three stages of a Disaster Recovery plan:

- Assess
- Adjust
- Improve

LXI offers comprehensive software and professional services to help customers achieve their business continuity goals. These services vary depending on the status of an organization's existing plan and available resources.

With LXI, customers gain the benefit of industry-leading storage management products and services for midrange systems.

Protecting corporate information infrastructure for more than ten years, LXI is focused on helping businesses manage their overall storage needs, including backup, recovery, tape and vault management, and data replication for high availability. Our professionals are dedicated to providing quality products, customer service, training and consulting services to help customers build and manage their information infrastructure most effectively.

LXI partners with such software and hardware industry leaders as IBM, Sun Microsystems, Hewlett-Packard, Computer Associates, TD Systems, and Maximum Availability to bring our customers the most comprehensive solutions available.

Disaster Recovery Planning

Are you prepared?

In all types of businesses around the world, CIOs, vice presidents, directors, managers and supervisors are asking their staff the same question: "Can we recover?"

The need for reliable data recovery has moved from just important (on the agenda at the next board of directors meeting) to both urgent and important (priority one on departmental managers' to-do list). Unfortunately, simply having a Disaster Recovery plan can provide a false sense of security.

Disaster Recovery—Planning for Business Resumption

Sitting on your desk is a four-inch binder. Inside that binder is everything you need to recover from a disaster: check lists, tasks breakdowns, phone numbers, and guidelines for executing your company's recovery plan. It's a good plan developed by many talented individuals who tried to think of every conceivable possibility.

However, inconceivable events have proven that standard assumptions about the level of damage, area affected, and regional consequences are not always enough. Having a plan to restore the data on a production server is meaningless if the personnel with the expertise cannot get to the recovery site.

Secondary communication plans can fail as communication utilities struggle to support the volume of traffic. Companies scramble to find office space, never dreaming they would have to compete for locations.

In short, the plan sitting on your desk may not be enough to guarantee your company's survival.

Expectations of data availability have changed. The Disaster Recovery plan outlines how to restore damaged or destroyed computer systems and the peripheral infrastructure needed to resume business operations after an outage.

The primary focus of your plan is business continuity—redirecting your users to the production data—as quickly and as seamlessly as possible.

The planning phase of any Disaster Recovery plan is most critical to ensuring your overall business continuity. The planning phase provides a blueprint for recovering from a disaster. Evaluating whether or not your recovery plan is adequate can be segmented into three steps:

- **Assess**
- **Adjust**
- **Improve**

Begin by assessing your current plan. The elements of the adjusting phase are crucial when adapting the plan to fit new technologies and business requirements. Then improve your Disaster Recovery plan for maximum effectiveness.

Assess: Where is your plan now?

The best way to be confident in your Disaster Recovery plan is to test it. Testing can involve contracting a recovery site service provider to utilize a specific configuration of computers, network connectivity, and facilities required by the plan or you may simply have a duplicate system — local or remote — that can be used as the test target.

Testing is a costly and demanding exercise, but the end results provide quantitative data and invaluable experience to everyone involved. Moreover, if the test fails to accomplish the goals, the failure can be analyzed and actions taken to correct the plan without placing your company in any further jeopardy.

Auditing your plan is less dramatic, but just as valuable. The practice of auditing a Disaster Recovery plan will be far less expensive than testing, but may require just as many man-hours. In the audit process, each section of the plan is scrutinized by an individual or group to determine if the defined action steps are:

1. Reasonable (makes sense).
2. Actionable (can be accomplished).
3. Within the scope and objectives of the overall plan.

An audit can be performed by your staff or outsourced to companies that provide audit services. Testing the plan can be scheduled or non-scheduled. In a scheduled test, all items and personnel needed are prepared ahead of time. In a non-scheduled test, the call to test the plan may come at a most inappropriate time and is more of a true test of a company's Disaster Recovery plan. One should always start with a scheduled test first to flush out any obvious omissions.

Adjust: How do you fill the gaps?

Regardless of how the plan is assessed, you will probably need to revise it. The need to reassess assumptions, requirements and expectations will become apparent. The rate of change in business today assures that business requirements will shift, new statutes will be adopted, and customer demands will increase. To be effective, the Disaster Recovery plan must address these changes by regularly challenging the assumptions, expectations, and constraints.

Instituting a change control methodology for your Disaster Recovery plan will accomplish two objectives. First, a formal process will have a better chance to achieve the desired results of an updated plan. Second, a formal change control process can also ensure that as requirements, equipment, applications, procedures, and personnel change, the Disaster Recovery plan will reflect those changes.

The goals and objectives of a Disaster Recovery plan must also be re-examined. Simply being able to restore critical data may have been replaced in importance by continuous up time, yet restoring systems and data remains a critical requirement. Based on the new underlying assumptions and expectations, new goals will need to be identified.

Management may now truly understand that an ounce of prevention is worth a pound of cure. Resources must now be expended to decrease the risk of system outages and increase the certainty that if an outage occurs, all the data will be recoverable. While there will be some expense involved, adjusting your plan does not have to be prohibitively expensive.

Options such as mirroring, remote backups, remote tape duplication, and automated backup strategies all require software and hardware reassessment.

RAID protected disk drives, SAN environments; automated tape drives and secondary systems are all safeguarding options. Redundancy, whether in data, hardware, or network are double the cost to maintain. As a result, companies must balance the need to reduce the organization's *risk* against the *cost* of services, equipment, software, and personnel.

Risk vs. Cost

How can Disaster Recovery planners reduce risk in the most cost-effective way? There is an inverse relationship between the "Risks" and the "Costs." As risks go down, costs go up. So how does the Disaster Recovery planner start?

You must first start with the things that can be controlled, beginning with the manual processes and procedures already in place. During your assessment, weaknesses may have been discovered. Correcting, changing, or implementing new process controls to address your company's exposure is the most efficient and cost effective way to reduce risk in a data center.

Good process controls are the key to a successful Disaster Recovery plan. No matter how much automation you have set in place, people still have the final responsibility.

Then review the fundamentals. If these essential disciplines are lacking or are not being followed, your Disaster Recovery plan is probably not worth the paper it is written on.

Security: How well are the current policies and procedures addressing the areas of:

- Physical Site — Locks, fire suppression systems, monitors.
- System Access — User profiles, passwords that change regularly, limited access to only applications and data needed.
- Network Access — Control and monitor internet browsing, email, and downloads, establishment of
- Firewalls.

Backup Strategy: How well are the requirements of the backup strategies being met for:

- Full Backups — snapshot of all data on a system to establish a starting point for recovery.
- Incremental Backups — Performed that only saved data that has been added or changed for a specific time period.
- Cumulative Backups — Performed that saves all data that has changed since the last full backup.
- Immediate replication for high availability.

Off Site Storage Strategy: How well are backup tapes protected?

- Locations — Defined places where tapes will be stored.
- Move Schedules — Where tapes are moved to and how long they will stay there.
- Slots/Containers — How the tapes will be stored in the off-site location.

Process Automation: How well does your current environment guarantee system activities occur on time and complete correctly?

- Activation — Recurring processes.
- Message monitoring — Error reporting.
- Event monitoring — Failures or abnormal completions.
- Access to drives.

These disciplines are not the only way to ensure recoverability. Other alternatives will provide more immediate protection, but also add significantly more cost as shown in Figure 1. Therein lays the ultimate challenge for Disaster Recovery planners, data center and senior managers: how to ensure recoverability without affecting the company's bottom line?

Improve: How do you find the right solution?

Reviewing the Options

Today, technology is providing cost-effective means to achieve your company's goals for fast recovery and continuous up time. High availability software is available that allows replication of data from one system to another across unlimited distances. Disk arrays provide similar mirroring functionality as software solutions, but with less flexibility. Storage Area Networks (SAN) utilizing fibre connectivity enable faster backups, non-disruptive duplication of data, and immediate off-site copies of backups across distances that were once cost prohibitive. The introduction of iSCSI (or SCSI over IP) allows backups to occur at remote locations utilizing the existing internet or Intranet networks. Each of these solutions can increase the recoverability of your organization's data, and each comes with a price tag that must be balanced with your overall budget.

So where to start? Management expectations and goals are a good place to begin. Direction for selecting new technology must be driven by the people that sign the checks. Conducting a review of the scope and objectives of your overall disaster recovery plan with senior management should provide the necessary guidance that will enable you to look for better ways to ensure recoverability.

For example, if certain applications or departments require continuous up time, you may want to investigate data replication solutions. On the other hand, if the review of your plan shows that regular backups fail to complete in the allotted time frames, you will need to determine if the problem is process, equipment, or the sheer volume of data. Each problem can be addressed using a single hardware or software solution, or by mixing and matching any number of these solutions.

Using the above example, if the problem is that the backup devices are old and slow, new tape technology can be introduced. If the problem is that the night operator forgets to start the backups on time, backup management products, automated tape libraries and automation products such as job can resolve the problem.

If the issue is that the volume of data to be backed up is greater than the time available, then solutions such as data replication software, faster tape drives, SAN configuration or simultaneous saves to multiple drives can meet the time considerations.

By evaluating the inadequacies of a disaster recovery plan, new alternatives can be found to meet and, in most cases, exceed expectations. Whether by software, hardware or procedure, weaknesses can be overcome.

Cost to Implement a Reliable Disaster Recovery Plan

Budgeting for Disaster Recovery is like buying car insurance. You want the most coverage for the least amount of money and you really would rather not have to pay for it at all. But like car insurance, a Disaster Recovery plan is a must have.

Which leads to this question: How much should a company spend on disaster preparedness? The answer is simple: It depends.

The amount of money a company spends on Disaster Recovery, Business Continuity, or Business Resumption is directly related to the organization's goals and expectations. Every company should have a documented standard regarding the acceptable amount of down time. It will be the responsibility of the Disaster

Recovery planners to meet or exceed that standard. Therefore, the cost will depend on how the company defines its standard. If the standard states that there will be 99.5% uptime, 24/7, in a single year that means that the system will be up for all but about 45 minutes. To achieve this, the Disaster Recovery planners and data center managers will have to implement technology solutions that ensure that in the event of an outage, users will be directed to backup systems using replicated copies of the production data.

Selecting Software Solutions

Looking at the fundamentals, the simplest way to be sure that basic data protection practices are being followed is to use automation tools. Implementing automation tools provides the capability to achieve security at both the system and applications level. Backup, recovery and tape management tools provide protection by not only backing up data but also preventing accidental re-use of media prior to its expiration.

Off-site management tools ensure that tapes are being moved and returned according to the corporations retention needs, and provide information about tape location for quick access. Data replication and mirroring tools provide quick availability to data for immediate access on a secondary system.

Selecting Hardware Solutions

Supporting the software solutions, hardware alternatives provide for faster processing and alternate backup or high availability solutions.

Automated tape libraries and storage area networks (SAN), or network attached storage (NAS), implementation increase the speed and efficiency of managing backups on a daily basis. For maximum availability and data redundancy, duplicating backups or performing data replication to an alternate system or backup media at a remote location provides for almost immediate access to secondary location when the primary systems have been damaged. The flexibility, scalability, and resilience furnished by these options add considerably to the recoverability of your business.

Do it Yourself . . . or Find a Provider?

At first glance doing it yourself appears to be less expensive than purchasing a software or hardware solution(s). Within your organization you have talented people that, given enough time, could provide excellent solutions, but having enough time is the determining factor. Spend 12 months developing and testing, or find the tools needed, and within 30 days improve the recoverability of your systems.

A Disaster Recovery plan encompasses much more than these basic process requirements. Highly successful companies recognize this and apply their resources to finding ways to simplify recovery through the use of available technologies.

What You Need to Know

While the number of vendors varies by platform, the criteria used to select products and services do not. No matter what tool you select, it must be able to support your Disaster Recovery plan and your organization's critical processes.

Listed are key considerations to remember in selecting a solution provider:

- Proven track record in meeting customer requirements.
- Experience in multi-platform environments.
- Ability to understand your business and your special needs.
- Integrated solutions that work well together.
- Focus on business solutions, with a good understanding of the big picture.
- Resources to support implementation, training and on going support.
- Commitment to providing worldwide support 24/7.

Bringing it All Together

Regardless of whether you call your plan Disaster Recovery, Business Continuity, or Business Resumption, you cannot afford to assume that the plan developed even a year ago is still relevant today.

Assess what you have, adjust to the identified changes, and continuously seek out newer, better, and more cost-effective ways to ensure that when the question comes from your superiors "Can we recover?" you can say confidently and without hesitation "Yes, we can recover -- and quickly!"

Assess
Adjust
Improve

To learn more how we can help your business recover, call 1-800-226-6526 or visit www.lxi.com

Our Commitment To You

LXI is committed to achieving 100% customer satisfaction. We fulfill this commitment by providing our customers with the most technologically advanced and operationally efficient enterprise solutions available. Protecting the corporate information infrastructure for more than ten years, LXI is focused on helping businesses manage their overall storage needs, including backup, recovery, tape and vault management, and data replication for high availability.

Thirty-day onsite demos are available for all of our solutions and are highly recommended so you can see firsthand how they function. Our professionals extend our commitment to you by providing quality products, customer service, training and professional consulting services to help customers build and manage their information infrastructure most effectively.