

EMC PERSPECTIVE

Getting Started with Disaster Recovery Planning

Ten Misperceptions, Five Best Practices

John S. Linse

Director, Business Continuity Services, EMC Consulting

Getting Started with Disaster Recovery Planning

Ten Misperceptions, Five Best Practices

Natural and man-made events plus the technology innovations of the 21st century have heightened awareness and dramatically changed the realities of planning for and implementing business continuity/disaster recovery (BC/DR) programs.

Although business continuity/disaster recovery remains equally or more critical than ever, many organizations are making decisions about whether or not—and how—to proceed with disaster recovery programs, based on outdated information and misperceptions about expense, resources, complexity, and logistics. Many who are considering this undertaking equate the task to “simply” buying and implementing storage equipment and replication software.

In reality, this component of disaster recovery planning should be one of the last steps in the process. Decisions about technology should be predicated upon a clear understanding of the business impact of an outage, current recovery capabilities, and objectives for improvement, and should be made within the context of a best-practices-based disaster recovery strategy.

This paper addresses 10 common misperceptions—and introduces five best practices—to help your organization get started on a successful business continuity/disaster recovery initiative.

Ten common misperceptions about business continuity/disaster recovery

- 1. Implementing a business continuity/disaster recovery program is expensive.** The cost equation of business continuity/disaster recovery has changed with the introduction of new approaches to recovery (e.g., asset reutilization) and new technologies such as server virtualization, data replication optimized to reduce network bandwidth, and automation tools that give you the availability benefit at less expense.
- 2. You have to do a business impact analysis (BIA) of everything in your organization, and that is a time-consuming, costly exercise.** A full-blown BIA could be overkill and can take months. Through interviews and discussions over a few weeks, you can gather enough data points to understand and isolate those things that you really need to focus on. For example, what business processes are most critical to bring back online during an emergency? What are your mission-critical applications? Who will be most affected by a disaster?
- 3. Disaster recovery only involves natural disasters.** While natural disasters may be the most visible and publicized causes of major outages and losses in the data center, the most frequent cause is power outages. Hardware failure and administrator error are equally culpable.
- 4. Backup data centers must be situated in another region.** There are many misperceptions about location and distance for establishing a backup data center—for example, that it must be hundreds of miles away or in another state to prevent losses from natural disaster. In fact, specific geographic location may be secondary to being on a different power grid or proximity to emergency staff. Unless industry regulations define specific parameters for backup data centers, your recovery objectives and alternative available power resources will help you determine the appropriate distance between data centers and the best physical location—which could be in or out of state, on the same property as the primary data center, or nearby, but on a different power grid, for example.
- 5. Tape-based recovery is still the cheapest option available.** Backup and recovery to tape may not be the most cost-effective method, especially if you have a large volume of data. It fails 12 percent of the time and doesn't scale well for performance and cost reasons. Recovery time grows linearly with the volume of data and may not align with service levels. Media costs also grow as the volume of data grows. Cost efficiencies and increased reliability can be achieved by using more advanced backup and recovery techniques for your most critical data and reserving tape for less important data.
- 6. Business continuity is an expense like an insurance policy—and senior management won't pay for "insurance."** How much you need to spend on business continuity/disaster recovery should be contingent upon your business risk profile and compliance mandates. Business continuity/disaster recovery involves governance, risk, security, and compliance, and activities should roll into your governance/oversight model or risk tolerance (for accepting risk). The business can then evaluate, based on that risk profile, how much to spend on business continuity and it becomes a business/cost tradeoff rather than a business decision made without this input.
- 7. Managing production in a failover site is difficult.** You can use a backup data center for production purposes. New technologies (e.g., virtualization) make it much easier to stage, manage, and decommission production workloads on a dynamic basis, reducing the management burden and making an active-active model feasible.
- 8. Business continuity/disaster recovery is only for your financial applications.** In today's world, e-mail, Web applications, and other data need to be recovered too, and in a much more robust fashion than five years ago. Furthermore, any company that has an ERP system, complex federated system, or large centralized database is actually at a greater exposure risk than organizations doing only financial transactions. These large database applications and complex federated systems are often the lifeblood of the organization and have an equal or greater impact on the business than financial applications if an outage occurs.

- 9. All you need to do is get budget and purchase hardware and software.** Buying and implementing equipment is one of the last steps in a business continuity/disaster recovery initiative and should be driven by many other prior decisions. Additionally, new processes, application tiering, and new technologies such as virtualization can improve utilization of and efficiencies with existing resources and can minimize the need for new product purchases.
- 10. If your data is replicated, you have a complete recovery plan.** Data replication is essential to any recovery plan. Without your corporate data, you would not be able to continue doing business as a company. There would be no recovery without a copy of the data. However, data replication is not the whole picture. The recovery of the server, the network, the security, the workspace, access to the systems by the users, and normal IT checks and balances all need to be part of the recovery approach and strategy.

As a just-in-time service provider of a vital community resource, Louisville Water Company (LWC) needed to ensure that its information technology resources could continuously operate critical business processes and recover from a disaster within acceptable downtime and information loss margins, at a cost commensurate with the risk and consequences of business process interruption. However, with four core business operations, 12 supporting operations, and over 40 business processes, management and staff expectations for business continuity/disaster recovery capabilities varied widely, and the need for an enterprise-wide BIA appeared inevitable. A business impact analysis questionnaire, focused on the core business operations level, allowed LWC business process shareholders and staff members to define their respective business interruption scenarios and operational/financial impact critical factors. Internal discussions on the documented responses facilitated consensus on critical business processes with the greatest operational and financial impact and their interdependencies throughout the organization. The process took just six weeks and enabled LWC to gain full buy-in, create a roadmap, and estimate funding for a new IT strategic plan.

Five best practices for successful business continuity/disaster recovery

The following best practices, proven through the development and real-life testing of multiple business continuity/disaster recovery programs, can help you build a roadmap and strategy and embark on a successful initiative without consuming your budget, resources, and management time.

- 1. Business justification.** Document your objectives and gain business buy-in to ensure that you have the support and financial backing to see your project through. Perform a business impact analysis to quantify, for targeted applications and organizations, the risk of an outage, current response plans, recovery-time objectives (RTO) and recovery-point objectives (RPO), and other information such as security and retention and archive requirements. Two key elements are the target outcomes:
 - Understanding the cost of an outage on a business process or application—this helps in making the business decisions around the level of investment that can be made to protect that process or application.
 - Developing a recovery priority among the applications and business processes—this helps put one application into perspective across all of the applications.
- 2. Recovery approach.** Before following industry best practices, consider your current real estate, computing assets, power consumption, regulatory and business requirements, and more to identify the right location and the right approach for your recovery data center. Match your recovery needs to the business impact of an outage. Develop a tiered approach for managing your recovery—not all applications are the same and not all are tier 1 applications. When developing a tiered recovery strategy, be sure to consider which are business-supporting versus business-critical applications. The tiered strategy should start with the characteristics of your recovery requirements (recovery-time objective and recovery-point objective) and include security, access, and data retention and storage considerations.

With the recovery requirements as a foundation, a reference architecture can be developed and then compared to the actual architecture resulting in a gap analysis. Knowing the supporting architecture of a recovery tier also establishes the basis for calculating the acquisition and operating costs for that tier, and leads to an understanding of the processes and procedures that will need to be updated to maintain that tier of recovery—ultimately giving you a complete picture from the business case to the operationalization.
- 3. Recovery objectives.** Recovery-time objectives and recovery-point objectives should be set based upon the results of the business impact analysis. The investment that a company makes to meet its recovery objectives should correlate to the outage impact that an application or business process has on the business—the more the business relies on an application or a business process (or supporting data), the greater the importance of that application. The amount of time that it takes to recover an application (recovery-time objective) is proportionate to the amount of money that will be spent to build the supporting architecture—the faster the recovery requirement, the more costly the solution. The same correlation holds true with the amount of data loss that is tolerable—the lesser the amount of data loss, the greater the cost of the solution.
- 4. Data management.** Data management is one of the foundational pillars of recovery. Develop a strategic approach for data management that includes independent considerations for disaster recovery, operational recovery, and archive; there is no one-solution-fits-all approach. Consider how you manage your data for each scenario—for example, archive it first to get it off the data store, replicate your data for disaster recovery, perform backups for operational recovery, etc. The better your data is managed, the better you will be at achieving your recovery objectives. Data also has a lifecycle that should be considered. Older data can be archived and removed from production. Backups should be done with a specific purpose in mind and should include a deduplication technology as part of the architecture.
- 5. Managing the recovery program.** There are two aspects of recovery—disaster recovery (the processes to restore the technology to the business users) and business recovery (addressing where people will go and how an alternate work location will be established). Both need to work for a business to continue operating when a disaster strikes. Managing the recovery program must focus on setting objectives for both of these recovery disciplines, measuring them against key performance objectives, and improving upon them on an ongoing basis.

EMC Consulting

As part of the world's leading developer and provider of information infrastructure technology and solutions, EMC Consulting transforms information into business results. Our consultants bring a unique mix of industry, business, and technology expertise to solve today's toughest challenges. We use field-tested tools, proven methodologies, best practices, and industry standards to minimize risk and optimize time-to-value in our engagements. We provide a full range of consulting, design, implementation, and support services. For more information, visit www.EMC.com/consulting or contact your local EMC Consulting representative.

Conclusion

As IT environments grow in complexity, so do the risks associated with ensuring continuous business operations. Are you confident that your organization is prepared for disaster? Many organizations assume that they have done due diligence because they have implemented the latest technology and believe they have an adequate understanding of their business needs for recovery, yet they find themselves woefully unprepared when an outage occurs. By understanding fundamental realities about expense, resources, complexity, and logistics, and by following the best practices outlined in this paper, you can define a sound disaster recovery strategy that aligns with your business requirements, resonates with your key executive stakeholders, and enables you to truly protect your business while remaining within acceptable budget and time parameters.

About the author

As Director of Business Continuity Services within the EMC Global Services organization, John Linse oversees EMC's Business Continuity practice, maintaining its relevance and value to customers. John's expertise and commitment to quality is exemplified by his leadership in disaster recovery and business continuity strategies across many industry verticals including healthcare and legal. Previously with Accenture, John holds degrees in Marketing and Accounting, as well as a U.S. Patent for an Electronic Bill Payment Device.



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com