

THREE RECOVERY EXPOSURES YOUR ORGANIZATION IS FACING – AND YOU MAY NOT EVEN KNOW IT

BY REBECCA LEVESQUE



Growth and profit – it’s the mantra of today’s aggressive business executives. With market pressures mounting and stockholder value in the balance, busy executives continue to seek unique solutions to customer challenges in an attempt to establish competitive differentiation.

However, the very drive and ambition that pushes your organization forward may be putting you at risk. Many company executives we speak to put so much energy into the development of innovative infrastructures and environments to provide better service and

greater customer insight that they forget about developing the strategies and tactics to ensure it can all be recovered.

The siloed approach separating business management and IT management often does not allow the insight into how IT departments are ensuring that critical business processes can continue after an event. Business managers don’t require a crash course in IT management to see how their applications and data are managed, but they certainly should understand the opportunities and exposures related to recovering those critical resources.

John Morency, a research director at Gartner, has noted that “for many organizations, time required to recover critical business processes...has dropped by roughly an order of magnitude from what it was 10 years ago.” We have seen similar trends; the business continuity market has notably shifted in the past few years, with greater focus on availability and recoverability, as well as intense interest in auditing and validation.

Identifying when and why

Data recovery strategies should contribute to operational efficiencies and business initiatives, as well as focus on shrinking recovery windows and aggressive Recovery Time Objectives (RTO)/ Recovery Point Objectives (RPO). Companies with truly effective data recovery strategies benefit from greater availability and reduced risks, as well as lower overall costs of recovery management. Effective data recovery strategies should provide a window into your actual application and data usage, and align your recovery management with real-world business challenges.

A business impact analysis (BIA) can help assess the business impact of data loss when a rapid recovery does not occur. However, it’s important to note that the static nature of a BIA can prove to be problematic, especially if the analysis involves a high degree of speculation. As such, companies run the risk of missing the full impact of potential disasters.

In today’s increasingly competitive and regulated marketplace, achieving an ironclad, dynamic data recovery strategy is the price of doing business. However, with the increasing costs associated with securing successful backup and recovery, accomplishing that goal is more difficult than ever. We believe that most recovery exposures can be separated into three categories; and if properly addressed, will significantly enhance recoverability.

1. 50% of all disaster recovery tests are unsuccessful

While most companies have documented recovery procedures for retaining and recovering information across the enterprise, those processes often fail during testing and real-life recovery efforts. According to Gartner, more than 50%

of all DR tests fail and 95% of all companies never complete DR testing. The primary reason for these failures is the lack of knowledge about physical and virtual systems, storage, applications and data, as well as their interdependencies.

In addition, many DR plans do not highlight the most critical and sensitive applications and processes that would be immediately required after an event. Therefore they do not prioritize those applications for immediate recovery so that the business can continue these operations. That means the critical applications and data you believe to be backed up and recoverable may indeed be a major exposure to your continuity.

Compliance requirements are often causing some of these challenges. Retention policies are often at the top of many compliance rules and audit requirements, and companies are turning to complex mirroring and redundancy efforts to ensure data is stored and secure. However, creating duplicate copies of all data also replicates any errors or corruptions. In addition, it can extend the time-to-recovery because all that redundant data needs to be recovered and restored – regardless of its importance or its impact on your business operations.

We always recommend a complete assessment of application and data interdependencies, especially as it relates to the most critical files and data your organization would need immediately following an event. That assessment needs to be very flexible, as the data sets you require on a quarterly, monthly and even daily basis may change often.

2. New technologies can actually increase your recovery risk

Many DR processes based on legacy systems have not changed in many years, so they do not include the newest applications and servers integrated to support new business initiatives. That means all the latest ERP, SFA or CRM applications you may have installed to improve customer insight or increase productivity may be at risk.

Applications and databases are often installed across multiple physical servers, and could be located in different physical locations. An event that disrupts the normal processing capabilities at

any location will put your new application at risk. However, because DR plans are often only updated yearly, you may not even know the extent of your current exposure.

Even worse, the implementation of new IT initiatives like consolidation and virtualization that are intended to reduce operation and management expenses may actually cost more in business loss and compliance fines later on. Virtualization, which offers tremendous benefits by separating applications

The implementation of new IT initiatives like consolidation and virtualization may actually cost more in business loss and compliance fines later on.

from their physical servers and providing greater management capabilities, can greatly reduce application recovery if not managed correctly. With many new and legacy application and data interdependencies scattered across multiple virtual machines, your ongoing recoverability is directly tied to your IT department's ability to track and manage those interferences.

3. Few companies can consistently prove they're recoverable

As we pointed out earlier, compliance regulations are causing havoc in the data center as well as the executive suite. Corporate and regulatory agencies often require proof that sensitive and critical data is recoverable as part of an overall compliance survey.

Most backup applications can provide a list of storage locations for backup data. However, focusing too strongly on auditing and reporting on data volumes – without obtaining access to the type of information that can provide real business value and insight – can prove to be problematic in creating a solid long-term business continuity plan.

That's why the only proof some organizations can offer is to point at their mirror site with all their redundant data and plead for understanding.

In the wake of compliance requirements and the competitive exposures that come along with them, executives and business managers should have the ability to prove that their processes and workflow are recoverable through audits and verification reports that provide reporting on demand. That means establishing a documented process for monitoring critical applications and files, tracking their backup location, and providing a critical path for the immediate recovery of those resources when needed.

So where do you go from here?

Below are some key areas of concern to ensure your IT department is aligned with your business requirements, and is able to recover critical applications and data when needed.

- Can you identify critical applications?
- Is your most important information recoverable in an acceptable "business window"?
- Are you maximizing the utilization of your storage resources?
- Are you using mirroring or replication to its greatest efficiency?
- Do you know what is missing from your recovery process?
- Have you tracked where all your data is by key process – and how you plan to retrieve it in the event of an emergency?
- How do you handle data corruption vs. technology or environmental disruption?
- Business managers and executives can work together with the IT organization to address these areas and close the gap to recovery.

ABOUT THE AUTHOR

Rebecca Levesque is Senior Vice President of 21st Century Software (www.21stcenturysoftware.com). She regularly addresses many DR/BC related user organizations and enjoys sharing the benefits of her experience and exposure to a multitude of DR issues. She has spent over 15 years in storage management and disaster recovery with hundreds of client companies.