Backing Up and Recovering Your Business Data: 10 Best Practices

Tim Burke
President & CEO
Quest

All your customer files have evaporated. As have everyone's email messages, all pending customer orders, and your accounts receivables database. Now you have to reconstruct that data from scratch. Or, worse, try to move on without it.

How much does your business rely on its data and digital applications? A recent study by Forrester Research and *Disaster Recovery Journal** shows that, on average, 72% of an organization's data and apps are either mission-critical or business critical.

No wonder a flurry of other studies have shown that so many enterprises — between 40% and 70%, depending on who's talking — go out of business after a significant data loss.

The reasons behind data loss vary — hardware/ software failure, human error, malware, natural disasters. But what all these reasons have in common is the fact that a solid data backup plan can prevent them from bringing your business to its knees.

10 steps to backups that really work

As I see it, there are 10 best practices that can make the difference between backups that really do keep you in business and backups that seem to work okay — until you actually try to use them.

1 Understand your data so you can decide what needs to be backed up and how often

Base your decisions on the cost of loss, which you can get a sense of by noting the types of data your business relies on — emails, spreadsheets, databases, line-of-business apps, etc. — and determining the impact of losing that information for good and having to recreate it (if you can).

Add in the cost of unhappy customers and potential regulatory/ compliance violations — and do the math.

2 Know your recovery requirements so you can prioritize which data needs to be restored first

Backing up your data does you no good if you can't restore the business operations relying on that data. How long can you function without customer apps and data? That's the length of your recovery window. What about payroll? Inventory? Email?

Once you figure out how long you can be without the data and apps driving key functions, you can determine how quickly these must be recovered. A dependable backup/recovery advisor can help you find the right balance between recovery and cost.

3 Make sure your backup/recovery strategy adheres to all governance and compliance rules that apply to your organization

Rules abound about data privacy, security, retention — and vary by industry and region. Look for a reputable advisor who has the experience needed to understand your compliance environment and who successfully completes SAS-70 Type II audits.

4 Encrypt your backup data

Opt for a backup solution that encrypts data both during transmission and storage — and conduct a search for any 'back doors' that might allow unauthorized viewing of your data.

5 Employ a reliable, trusted remote backup service, so your data is housed in a secure remote location

Remote data backup has never been more affordable or effective, thanks to the convergence of several efficiency-enhancing technologies. Now it's possible to engage an online backup service that makes easy work of scheduling your data backups — or even automatically updating your data in near-real time. A couple of approaches are worth noting:

Backup in the cloud. Cloud backup has become increasingly practical and cost-effective, thanks to high-speed Internet connections, virtualized data center infrastructures, and deduplication, which eliminates data redundancy and thus reduces data volumes. Look for a provider who will support a local cache or can put copies of your servers' backed-up data on an appliance in addition to the cloud; this will speed up restores, notably database restores.

Data replication and vaulting. Mirroring your data at high LAN/WAN speeds to one or more electronic vault environments keeps your data continually updated in a secure remote location — and enables quick recovery. You'll want a service provider able to replicate, vault, and restore both your mission-critical data and the applications (such as Microsoft Exchange, Microsoft SQL Server, Oracle) that use the data.

6 Back up your data locally as well as remotely

Data restores usually are faster from a local backup source than a remote one, especially for data that you recover frequently.

7 Secure your IT infrastructure to minimize data corruption and theft

You'll want to keep your firewall enabled unless there's a very specific and valid reason to disable it, and you need to ensure that all your malware defenses are always up-to-date (to make sure, I highly recommend automatic updates).

8 Don't forget: Data backup/recovery is key to your ability to recover from disasters and sustain business continuity

The planning and implementation of your backup and your DR/BC efforts should be tightly integrated and reviewed at the same time. Here, too, a trusted advisor can help.

9 Assign the management of your organization's backup/recovery efforts to a "Backup Czar"

Your Backup Czar should be responsible for ensuring that your organization's data and apps are backed up according to plan. Your Backup Czar also should regularly test *all* of your backup/recovery processes and conduct plan reviews to make certain those processes keep pace with changes in technology infrastructure, regulations, and business operations.

10 Conduct regular testing and reviews of your data recovery capabilities

Backups can be corrupted (especially if they're tape-based) and too often backups are performed incorrectly. Key files, directories, or components may have been excluded, especially if your infrastructure has undergone adds or deletes.

So you and your Backup Czar need to test your data recovery capabilities often and review your data backup strategy at least annually (quarterly is better) to make sure your backup/recovery capabilities are keeping up with your business.

6 ESSENTIALS TO LOOK FOR
in a backup/recovery services provider

> *Cloud backup/recovery via a secure virtualization-based datacenter infrastructure*

> *Data replication/vaulting services*

> *SAS-70 Type II certification*

> *Ability to integrate a range of backup/recovery and business continuity services*

> *Security-focused regulatory compliance and archiving services*

> *Complimentary assessment of your organization's backup/recovery needs*

Data backup has never been more important

As you explore which backup/recovery solutions will work best for your business, take the time to find a provider with leading-edge infrastructure and technologies as well as the skill and experience to keep your data safe and secure.

Make sure your provider knows how to deal with backup/recovery technical complexities so you don't have to. And perhaps most important of all, you'll want a provider who is both willing and able to understand the needs of your business and design an affordable backup/recovery solution just for you.

* *Disaster Recovery Journal: The State of Disaster Recovery Preparedness* (http://www.drj.com/2011-articles/winter-2011-volume-24-issue-1/the-state-of-disaster-recovery-preparedness.html)

ABOUT QUEST

One of the nation's leading technology consulting and management firms, Quest provides Professional, Managed, and Cloud Services in virtualization, security, business continuity/disaster recovery, data storage and colocation, networking, telecommunications, wireless, and technical staffing either on-site or from its secure nationwide service delivery centers.

Visit us at www.questsys.com.