

# Fine tuning corporate data protection

Disaster recovery plans are like insurance policies says John Sacke. It takes a disaster to recognise their true value. Who wants to be caught without one?

After the devastation of Hurricane Katrina in the US and other more recent global crises, businesses have been pursuing disaster recovery (DR) and business continuation strategies in earnest. The result is many more companies today are better prepared than they were two years ago. However, some traditional DR pitfalls remain.

This is because DR plans operate on the backburner when everything is going well and take centre stage when the company is flung headlong into disaster. Most of the time, DR does not gain the ear of high-level executives until a business interruption strikes. The planning and the execution of data recoveries are orchestrated by mid-level personnel in IT and business operations.

The bottom line: disaster recovery plans operate like “insurance policies” that only become valuable when a company runs into disaster – although industry regulators, legal experts and others have now placed new demands on sites.

“Some of these regulatory demands are in areas like data retention and archiving, especially with the growing importance of email and data retention in compliance and litigation,” says president and CEO of Storagepipe Solutions Steven Rodin. Storagepipe Solutions is a US-based online backup, recovery and data protection firm. The challenge is finding internal IT staff qualified in new areas of data protection that regulators are looking for – whether it is backup/recovery or archiving.

“We still see an IT skills shortage, very acute in the area of data protection,” says Steven. “Especially in small and medium sized businesses, individuals are arbitrarily assigned the responsibility for DR – but they have no



The buildings may have insurance protection but what about the data they house?

specialised training for it. SMBs are overloaded and they also have smaller staffs. It’s easy to see where data protection and disaster recovery can fall to the bottom of the to-do list.”

## Current corporate readiness

Steven says his company gets many calls from SMBs and from large enterprises tasked with backing up, restoring and maintaining the data of many remote offices. By outsourcing to a company specialising in backup, recovery and archiving, these businesses can focus on their day-to-day activities without worrying about business interruptions if and when they occur.

“Regardless of company size, there are some major areas in data backup, recovery, archiving and protection that are still evolutionary,” he says. “For instance, most companies have not taken the approach yet to separating their

information into data that is absolutely mission-critical and must be instantaneous – and older data that should be archived – and obsolete data that should be purged. Consequently, we see companies expending more resources and backing up more data than they should.”

Steven says any corporate storage management strategy should address data archiving as well as backup and recovery. This is because industry regulators are demanding companies retain their data for longer periods – and regulatory and legal requests require this data is easily accessible, in near real-time.

Hurricane Katrina made it easier for corporate IT in North America to solve an age-old problem – getting a budget commitment from corporate management to go after traditionally ‘invisible’ projects like disaster recovery. Katrina also made the

scenario of high-level executives assessing damages to their businesses and having to talk to stakeholders and the press about what was going to happen, painfully realistic.

Once the DR money is spent, and new DR strategies have been implemented, how does the CIO go back for additional investment in data protection?

The answer rests in the areas of return on investment and risk management, coupled with higher expectations from industry regulators.

“Companies constantly ask us about what they can realistically expect in ROI,” says Steven. “We tell them they can start by projecting that they can save 30-50% off the top of their existing operational processes for backup, recovery and data protection when they outsource because they’re no longer required to purchase, lease and maintain backup software and hardware resources.

They also eliminate operational expenses for tape pickup services and other related charges to backup, recovery and storage of data. The IT staff manpower needs for backup, DR and data protection are greatly reduced. IT also has help in mitigating the current knowledge gaps on their staff.”

Steven says SMBs often look for an affordable turnkey solution, which makes outsourcing those functions very attractive. Even large enterprises look for outsourcing assistance in DR and data protection, because they have many satellite offices and facilities that must have localised disaster recovery and data protection plans.

“We often find enterprises are challenged to maintain current backups for their remote offices and locations,” he says. “They ask us to provide online backup and recovery services for these sites, and we respond by providing

state-of-the-art services that seamlessly mesh with their overall corporate disaster recovery data protection. We give these organisations comprehensive reports of all data backup, recovery and protection activity. Since we cover virtually every piece of hardware and software in the IT environment, from mainframes to end-user devices, we can also provide data backup, recovery and protection services to enterprises that include the corporate data centre.”

In the US, new regulatory and risk management pressures now call for advanced data protection that involves the integration of data archiving with online backup. Point-in-time data snapshots are required for compliance. Data archiving and retrieval might have to support a data ‘shelf life’ of up to 30 years.

To address the challenge, many



## Are your cablers registered?

Have you checked that your cabling sub-contractors hold a current Telecommunications cabling registration card? If not, you may be exposing your business and yourself to unnecessary risk. All cablers (including electricians) are required by law to be registered to work on wiring for business systems, phones, faxes, building automation, fire/security alarms, internet, computer and data cabling.

All registered cablers are required to undertake appropriate training to ensure that they are competent to perform the cabling work according to the Wiring Rules (Australian Standard AS/ACIF S009), which ensures safety to consumers, cablers and the network.

So, make sure that your legal and insurance obligations are met! Only use registered cablers.



**Australian Government**

**Australian Communications  
and Media Authority**

**For more information visit  
[www.acma.gov.au/cabling](http://www.acma.gov.au/cabling)**





Find out  
more about

Smart Wiring™

in a

Telstra Velocity™

Development

**Telstra**  
Smart Community®

Visit our website  
[www.smartwiredhouse.com.au](http://www.smartwiredhouse.com.au)  
to download the Smart Wired™  
Functional Specs and the  
Features & Benefits flyer.

companies are keeping more data offsite. In an online offsite storage strategy, vendor-stored data is controlled with an additional layer of security and most likely a different security protocol from what the client company uses. This adds protection to the data. At the same time, businesses avoid corrupted data - or people internally deleting or manipulating data. Offsite storage vendors also typically encrypt data-while most client organisations do not.

"We work with clients on their audits to ensure absolute compliance - irrespective of the regulatory guidelines," says Steven. "Security is always critical. We use Tivoli software for backup, recovery and data protection, along with our internal expertise and practices to ensure the highest levels of security possible. For our clients, we offer an authentication model built on a challenge and response mechanism that confirms user identification and access privileges. We even have customers who prefer a direct connection strategy for their IP communications using T1 lines that circumvents standard IP-based traffic. We can use virtual private networks (VPNs) and government grade AES (advanced encryption standard) encryption, depending on the client's needs."

#### Best practices for data protection

The demands of regulators, real world threats, and virtual world threats like Internet breaches and data compromise have alerted most companies to the need for strong data protection and archiving methods that go hand in hand with disaster recovery. Nevertheless, the challenge remains the same: freeing up the necessary people internally to work on these issues - and ensuring they have the right training to do a job that is relatively new.

Following are four key recommendations for data protection for your clients (and your own business):

1) Define the data to be archived as well as your real-time backup data. A reputable outsourcer or consultant will have analytic tools that can help you determine which data is needed on a daily basis, and which can

be archived. If you do not have a clear idea on what should be archived, check with the consultant or service provider. Frequently, they have experience they can share to help you sort through data and define a strong archiving strategy that will complement your DR.

2) Email retention requirements have grown as email has become more important for the compliance, the discovery and the litigation processes. Most companies now have policies governing email retention, with a majority settling on a retention length of seven years. Make sure your company (or clients) has these policies in place - and that they are thoroughly communicated to all employees as well as to IT.

3) Regularly test data backup and recovery. These tests will help you quickly identify and plug any holes in your backup and recovery.

4) If you work with an outsourcer, be sure to clarify your RPOs (recovery point objectives) and RTOs (recovery time objectives) upfront. Most customers prefer a nightly RPO, but others require RPOs several times daily, and still others require realtime, continuous data backups for their businesses. These expectations should be central ingredients in your SLA (service level agreement) with the vendor. "Also, check references," says Steven. "Even if an organisation has a strong SLA, you need to trust the people whom you are dealing with. The SLA should meet your needs for data protection, hardware and software at the vendor site that is of enterprise class - because the outsourcer should be able to grow with you, and to be able to support a diversity of platforms." ■

*John Sacke is founder and president of Sacke and Associates Inc based in Toronto, Ontario, Canada. He has 14-plus years in consumer technology, has a bachelor of commerce and an intimate knowledge of media and analyst relations.*

#### CONTACT

Storagepipe Solutions

[www.storagepipe.com](http://www.storagepipe.com)