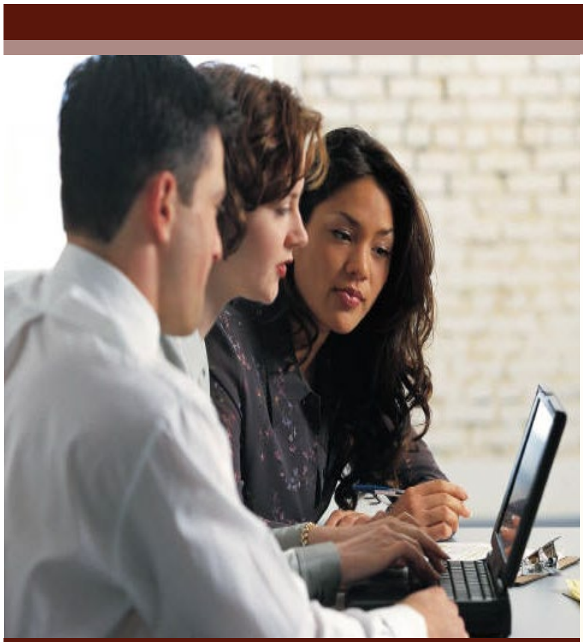
10 Backup Best Practices White Paper

How to supplement a disaster recovery and business continuity back-up solution with the cloud



CIO Support Solutions

- Disaster Recovery
- Business Continuity
- Security
- Compliance – ISO HIPAA SOX
- IT Strategy
- Job Descriptions
- Infrastructure
  - Artificial Intelligence
  - Omni Commerce
  - BYOD
  - Mobile Computing
  - Blog
  - Social Networking
  - Record Management
  - E-Mail & Electronic Communication
  - Service
  - Electronic Forms
- Metrics
- Safety Program
- HR Tools
  - Hiring Kit
  - Interview Guides

10 Backup World Class Best Practices

How to supplement a disaster recovery and business continuity backup solution with the cloud

Many CIOs want to improve their ability to recover from system failures and data loss, especially to protect themselves from natural like Sandy and manmade disasters like a terrorist attack. Building a disaster recovery and business continuity infrastructure is cost prohibitive for many organizations, thus the cloud is a perfect solution. The cloud can supplement an enterprises backup disaster recovery and business continuity backup solutions.

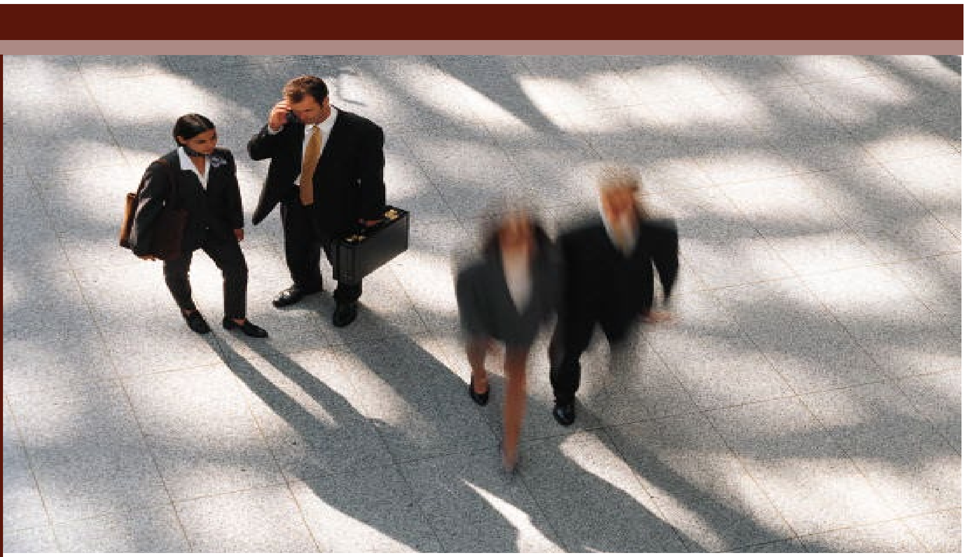
That being the case here are 10 backup best practices.

- **Local back-up is the first line of defense**. As Sandy proved when it comes to performing backup and recovery, the best performance will be delivered by using resources local (on-premises) to the systems and data being protected. However, in an extended outage you need the cloud like Sandy if power is out and the data center is down a more extensive solution is required.
- **Know the systems and the dependencies when the data center is down**. Local backup does not work when the data center is out of commission, then a cloud-based backup is a necessary second line of defense. You should know which servers and data that organization's day-to-day operations will need when the data center is down. Make sure they are protected with a cloud backup and restore.
- **Go beyond traditional backup for disasters**. Consider the ability to use replication technologies to provide continuous data protection locally and in the cloud, for critical systems. Replication, although a great complement, is never a replacement for backups. Even high availability software solutions can be used with a public cloud for automated and push-button failover for the most critical systems and applications.
- **Know what is required to restore data and back up to keep the business operating**. Backing up the system and all the storage will protect everything on that OS instance, which is perfect for when you need to restore the entire environment using bare metal recovery scenarios. If you are protect- or even a single email—so think about what you might want to restore then make sure you are backing up in a manner to facilitate your goals.
- **Backup may not be enough**. If a virtual server fails, all VMs on that server are at risk.
- **Minimize long-term backup cost**. Maintaining long-term disk-based backups on a company's resources can be very costly; maintaining long-term backups or archiving old or infrequently used files in the public cloud can be a great, cost-effective alternative solution for many organizations.

Janco's Business Continuity Template is the Industry Standard

The essential tool for organizational resilience and survival. It is the ideal for business continuity practitioners seeking :

- State of the art presentation of the global body of knowledge for DR/BC, including current international standards and best practices.
- Flexible, modular design that allows you to create a customized business continuity plan: Provides real world text with clear definition of fundamental principles and practices; Detail on Information Technology and Emergency Management for those focusing in these areas; a 20 page Business and IT Impact Questionnaire; and a detail work plan, business impact, and business continuity management, which is task oriented. Both the Business Continuity Planning Organization and the IT Productivity Center (ITPC) have endorsed the book.
- Quick reference for your business continuity team offering a readable blend of academic principles and practical applications—an effective tool for grounding interdepartmental teams developing and maintaining BCP plans.



Continued

- **Manage the security of cloud-based data**. Securing your organization's data is a major verify the security used in the solution—for example, the physical security of the public cloud locations, encryption of data at rest on the storage, and logical separation of your organization's data from other organizations using the same public cloud backup provider.
- **Run the recovery directly in the cloud**. Look at options to run your systems in virtual environments in cloud virtual machine hosting solutions using the systems and data backed up in the public cloud. This approach allows your operations to be up and running again even without your own datacenter.
- **Have a unified backup and management**. Most organizations that leverage a cloud for solution that supports a hybrid model and enables a single management approach.
- **Test the processes**. The best solutions in the world will fail if you don't know how to use them correctly—and if you don't perform regular tests to ensure restore processes work and the data protected is valid. Get into the habit of performing regular tests.

Cloud Disaster Recovery and Security Bundle

IT managers have eagerly implemented cloud applications to reap its many benefits: lower hardware and energy costs, more flexibility, faster responsiveness to changing and new applications, and improved resiliency.

But when disaster strikes, some IT managers find their disaster recovery techniques and hardware configuration have not kept pace with their changed production environment, and they're stuck, along with their recovery times, in the pre-cloud era. They falsely believe the improved day-to-day resilience of their cloud environment lessens their need for disaster recovery (DR) planning. In fact, the opposite is true: Catastrophic hardware failures in the cloud environments bring down many more applications than in non-virtualized environments, making DR planning and implementation more critical, not less.

Go to http://e-janco.com/clouddisasterrecoverysecruity.htm to see more

CIO Infrastructure
and
Management Tools

Disaster Recovery / Business Continuity and Security Bundle

It goes without saying that every company, regardless of size, needs a concise business continuity plan in case of an emergency. If you don't have a disaster recovery plan or haven't updated yours recently, now is the time to take this critical step to protect your business.

At the same time there are more security requirements that need to be met. With mandated requirements like Sarbanes-Oxley, HIPAA, PCI-DSS, and ITIL, executive management is depending on you to have the right security policies and procedures in place.

Go to http://e-janco.com/drp_and_security.htm to see more!

Best Practices for IT

Janco Associates, Inc.

Park City, UT 84060

+1 435 940-9300

support@e-janco.com
e-janco.com