

BEST PRACTICES FOR PROACTIVE DISASTER RECOVERY AND BUSINESS CONTINUITY

How to plan, implement and execute a quick recovery strategy for local accidents and natural disasters

EXECUTIVE OVERVIEW

Today's unpredictable world puts pressure on IT departments to maintain business continuity in the face of many challenges—natural disasters, network outages, cybercrime and security breaches can bring business to a halt if a company lacks a sound disaster recovery plan. However, with the right people, processes and technologies in place, companies can withstand and recover from even the biggest threats. In this paper, Dusty Williams, CIO of restaurant conglomerate OSI Restaurant Partners, LLC, and Mike Cybyske, CBCP, Manager for Qwest Disaster Preparedness review their experience with implementing disaster recovery plans in their organizations, and best practices for maintaining business continuity in face of natural or manmade disasters.

Our goal was to be up and running within 8 hours," he said. "With our DR plan in place, we can be up and running in under 3 hours.

Dusty Williams, CIO of OSI Restaurant Partners, LLC

DISASTERS HAPPEN. ARE YOU READY FOR THEM?

Are your business network and your IT staff prepared to deal with the unthinkable? Imagine for a moment what would happen if your network and all the systems and applications that rely on it were suddenly unavailable. With today's secure, highly available and redundant hardware and software solutions, you may have developed a false sense of security. But outages can happen. Consider these examples:

- In 2000, two major mobile equipment providers relied on the same outsourced manufacturer to provide a chip that was a critical component in the development of their next-generation cell phone. The chips were manufactured in Albuquerque, New Mexico. That year, a single bolt of lightning knocked out a cooling fan in the manufacturer's data center, started a small fire and burned some circuitry that was required to make the chips. One company had a backup supplier and was able to go to market with a successful cell phone product, while the other's lack of a backup provider caused their market launch to be delayed.
- Bell Canada experienced its worst outage in history in 1999 when a contractor dropped a tool on some electrical equipment at a switching location. A fire spread quickly, damaging equipment, activating the sprinkler system, and disrupting both commercial and emergency power supplies. The situation caused residences, businesses, banks, ATMs and hospitals to be without their communication network for several hours until crews responded and repaired the services.

No matter how solid your infrastructure, local accidents and natural disasters can happen, causing big problems in a short amount of time. Making sure your business keeps running despite the unexpected requires solid Disaster Recovery (DR) and Business Continuity (BC) strategies that go beyond redundant components or storage backup.

WHAT ARE DISASTER RECOVERY AND BUSINESS CONTINUITY?

How fast can you recover after a disaster, and how you keep business operations going while you're recovering is referred to as Business Continuity. Of course, this all depends on the strategies you have in place to either prevent a business disruption or to quickly resume a function that is disrupted. Sometimes called crisis management or disaster avoidance,

Disaster Recovery is not just the process of replacing or fixing the physical hardware in the data center, but having in place the people, activities and communication strategies necessary to maintain Business Continuity despite a natural disaster or local incident.

First let's consider what types of disasters can disrupt your business. Natural disasters like earthquakes, hurricanes, floods or lightning storms are the most obvious, and depending on where your business is located, may or may not be big threats. If you are in an area prone to natural disasters, you are probably aware of the potential danger and have enacted appropriate DR plans. Typically, however, there is an interest in DR solutions only following a hurricane or other major natural disaster. Unfortunately, this is a reactive approach, and most businesses are already affected by the time they begin to think about implementing effective DR strategies.

However, even if your location is safe from severe weather or shaking ground, other threats loom large. Extended power outages, water main breaks, viruses and technology failures can be worse than natural disasters in some cases, causing business to come to a halt indefinitely. In fact, most power outages are caused by on-site accidents, not natural disasters. Since 2001, the cost disruptions caused by viruses and cyber crime have increased exponentially, and as we become increasingly reliant on computers and technology, the people bent on capitalizing on that trend won't go away. To be fully prepared, businesses must begin taking a more proactive approach to handling these disruptions before they occur.

OUTBACK STEAKHOUSE DODGES DISASTER

OSI has implemented a solid solution for DR and BC and by doing so, avoided an 8-hour blackout in 2004 that could have cost the company its solid financial standing and reputation. A conglomeration of eight different restaurant concepts, OSI maintains 1500 restaurants in 49 states and 20 countries. Its main data center is in Tampa, FL at the company's headquarters, so hurricanes are a constant worry. Moreover, the data center has experienced flooding and fire, and sits just 800 feet away from the end of the main runway at Tampa International Airport. The IT organization supports all hardware, applications, networking and telecommunications for all OSI restaurants around the world, a task that puts tremendous pressure on staff to avoid downtime.

Understanding the importance of BC and the need for a solid DR plan, Dusty Williams, CTO of OSI began working with Qwest in 2003. He built a case for DR to present to the executive team, comparing the plan to an insurance policy. Already, there was leadership apprehensive about potential for frequent power outages and loss of network connections at company headquarters, so it was relatively easy to convince them that the company needed to take action.

Williams and his team selected Qwest CyberCenter Services to provide its DR solution. His goal was to set up diverse locations, but minimize flight time and cost between the locations. Qwest helped OSI implement a single network platform complete with 24x7 technical expertise, managed firewall services and DR at Tampa. A separate DR data center was created in Chicago. The data centers met OSI's requirements for power redundancy, data center availability and proximity to major internet PoPs for reliability and performance.

According to Williams, it took roughly 18–24 months to fully implement the solution. But now, he is confident that should disaster strike, they'll be back in business quickly. "Our goal was to be up and running within 8 hours," he said. "With our DR plan in place, we can be up and running in under 3 hours." And the completion of the DR plan was timely. "When hurricane Charlie was tracking to come through Tampa in 2004, the city of Tampa informed us they were shutting down the power grid that covered the area," he said. "If we hadn't already implemented our DR plan, we could have been dead in the water for an entire day."

AN EMPHASIS ON TEAMWORK, CROSS-FUNCTIONAL SUPPORT

DR is of paramount importance not only for Qwest customers like OSI, but for Qwest's own operations. As the leading telecom services carrier in the U.S. with a state-of-the-art, nationwide fiber optic network that includes 15 integrated hosting centers, recovering quickly from disaster is critical. To that end, Qwest has developed a framework that enables

multiple groups to work together to support incident response. The solution is flexible and addresses all the tactical issues associated with keeping critical functions going. A “crisis management” group consisting of executives from across the organization coordinates across business units to bring the right resources to the table for rapid recovery.

According to Mike Cybyske, CBCP, Manager for Qwest Disaster Preparedness, the real challenge of implementing a DR and BC solution is telling people what they don't want to hear. “You're asking them to spend money they don't have to prepare for things they don't think will happen,” said Cybyske. “The solution is to educate leaders, build support and set realistic expectations. We have to educate them on the risk and how their operations will be impacted.” The crux of the issue, noted Cybyske, is to bring all the pieces of data—threats, impacts, risk tolerance, financial situation—and synthesize them so that the solution is sustainable long-terms

BEST PRACTICES FOR A SOLID DR AND BC PLAN

Qwest has adopted the National Fire Protection Association (NFPA) 1600 standard for disaster emergency management and BC program, which provides specifications for:

- Full-time and part-time BC managers
- Critical function plans
- Application DR plans
- Data center failover
- Plan testing

In addition to these standards, here are some best practices to consider:

- **Know your priorities.** If you don't focus on what is most critical and prioritize, you'll be fighting an uphill battle.
- **Remember your suppliers.** The popular trend toward outsourcing provides most businesses with the option of offsetting workloads so you can still meet customer needs while you're recovering. Make sure you know who are the vendors and partners that support your business. Consider your supply chain for daily business operations, and have a backup-plan. Also, validate that your suppliers can do what they say they're going to do in case of disaster.
- **Keep planning.** Keep an eye on your changing environment and stay informed about what types of applications you need to continue to plan. Make sure new employees familiarize themselves with the plan as they come on-board. Being proactive is also essential. If there is a large-scale disaster, it can be difficult to get staff back in the area to take care of the issues that occur, particularly if you're working for an infrastructure provider or bank, where the pain is severe and immediate. Work with state agencies now to determine necessary credentials and processes to get people back into damaged areas quickly.
- **Communicate.** During a disaster, buildings are evacuated and people may scatter. It can be difficult to locate the people responsible for executing your DR plan. Have in place a simple, effective way to communicate with all parties — one that will not be affected by the outage. Make sure department heads maintain up-to-date contact lists and have a centralized number that employees can call for information. Use new forms of communication technology, such as text messaging, to disseminate critical information, if needed.

CONNECT. SIMPLIFY. ENHANCE.®

with Qwest Business Solutions®

Qwest is focused on helping you work smarter, with services that leverage the latest technology and award-winning support. Here are a few solutions that can address the issues covered in this solutions brief:

see over



QWEST IQ® CONNECT

iQ® Networking. Converge your legacy frame, ATM and private line data networks to a single MPLS or VPLS-based meshed, fast re-route environment. iQ Networking includes public Internet ports, private and mobile/remote connections, security, and management options. Reduce maintenance and management expenses while improving the performance of your network, and transition to new technology at your pace.

Hosting Solutions. Augment your data center space and IT infrastructure capabilities with Qwest's Colocation and Managed Hosting services. Locate some or all of your servers in secure, state-of-the-art, Qwest CyberCenter facilities with direct connections to the OC-192 Qwest® Macro Capacity fiber network. From basic colocation and managed hosting to storage and managed backup, Qwest can ensure your data is secure and always available.



QWEST IQ® ENHANCE

Business Continuation Routing. Business Continuation Routing (BCR) is an AIN based call forwarding service that allows a business to reroute their incoming voice calls to an alternate site, or to individual alternate telephone numbers in the event of an emergency. The primary intent is to provide customers with the ability to develop and pre-program a disaster recovery capability.

Data Circuit Reroute. COMMAND A LINK™ from Qwest is a network reconfiguration service that allows you to manage your communications system without assistance from Qwest. COMMAND A LINK™ can be used for network planning, data backup, peak data solutions, backup site sharing, access to time share or inter-exchange companies.

Remote Backup and Storage. Qwest® Storage and Backup Services provide Qwest Dedicated Hosting customers with a scalable, cost-efficient suite of data storage solutions that are tailored to your storage needs. Take advantage of Qwest Storage and Backup Services to enhance your disaster recovery strategies, back-up data and retrieve, restore and archive your data. Qwest Storage and Backup Services are secure and designed to grow with your needs.

SONET Route Protection.

- Self-Healing Alternate Route Protection (SHARP) is an optional feature of Qwest's Private Line DS1, DS3, and SST services that answers your need for assurance of system reliability in the local loop.
- Point-to-point transport
- Designed for moderate to heavy volumes
- Establishes two physically separate routes for the working service path and the protect path
- On SST, SHARP is available at the system level and 30151, for example, OC3

WHY QWEST

Qwest delivers reliable, scalable data and voice networking solutions, across one of the largest U.S. fiber footprints. Qwest serves businesses of all sizes, ranging from small business to 95 percent of Fortune 500 companies, with industry-leading SLAs and world-class customer service.

LEARN MORE

For more information about Qwest voice and data services for large businesses, visit www.qwest.com/business or call (877) 816-8553 to speak to a Qwest representative.