

# Planning for disaster and everyday threats

## How to protect business-critical functions and mitigate risk

From downtime costs to regulatory compliance, the need for strategic business continuity and disaster recovery (BCDR) planning is clear, but what does that mean for your organization? Mike Cybyske, a disaster preparedness specialist and crisis manager for CenturyLink™, says business continuity management (BCM) requires the ongoing assessment of risk to your organization. In this interview, he provides insights and advice for implementing an effective plan.

**Q As a business continuity expert for a large business, what are your top recommendations for customers looking to implement a BCDR plan?**

**A** Recognize that you can't protect everything. It's important to identify the business-critical functions and who is critical to supporting your business. Know what your critical functions, vendors and suppliers are and what you would stand to lose if they were unavailable for a few hours, a day or weeks. Then create continuity plans for those that you cannot afford to be without. And remember that it's not just hurricanes, tornadoes, fire and other disasters that can cripple a company. There are far more common events like bad software, misconfigured networks, hardware failures such as a bad disk drive or power outages.

**Q What are the common challenges that businesses face when implementing BCDR solutions?**

**A** One of the biggest challenges is getting leadership to spend money they don't have to prepare for things they don't think will happen. You have to educate leaders, build support and set realistic expectations. You have to educate them on the risk and how their operations will be impacted. And you need to focus on bringing together all the pieces of data—threats, impacts, risk tolerance, financial situation—and then synthesize them so that the solution is sustainable long-term. Trying to implement a corporate-wide program from the bottom up or individually within each business unit is difficult. An effective program requires a strategy that incorporates all departments and their participation from the top down, which can only be accomplished when corporate leadership understands and supports continuity planning.

**Q What are some of the primary elements of creating a BCDR plan?**

**A** A good plan should address four key elements: building, systems, equipment and personnel, plus contingencies for the loss of any or all of them. This multi-hazard approach allows flexibility in responding to the disaster and reduces planning redundancy since it is not event-specific planning (hurricane, tornado, winter storm, etc.).

**Q How have the risks a company may face evolved over time?**

**A** One risk that every company faces is changing technology. As corporations adopt technology to increase productivity or reduce costs, its impact on business continuity is often an afterthought. This can create gaps in a business unit's recovery and continuity strategy, requiring new processes to be developed and tested. This is especially true when different platforms are required—mainframe, virtual environments, Cloud computing—since different skill sets are needed to manage and recover each.

Contact your CenturyLink Representative today!



**Q Can you tell us about a time when you put a BCDR plan into action and what the result was?**

**A** Hurricane Ike caused an estimated \$38 billion in damages and a power outage that affected more than two million people in three states. Network equipment was undamaged by the hurricane, thanks to the layers of redundancy CenturyLink builds in to mitigate the impact of power outages on our equipment, and generator-based power kept the equipment operational. The challenge to business continuity came after the event. The power outage was prolonged and required us to secure fuel through multiple suppliers. Business continuity was maintained, and we strengthened the BC program by developing new supplier relationships, which may be key to business continuity in the future.

In early January 2009, Washington State experienced some of its worst flooding, mudslides and avalanches on record. More than 30,000 people were urged to evacuate their homes. Our primary concerns were the protection of infrastructure and the continuation of telecom services, including 911, to hundreds of thousands of customers. Plans based on historical probability played a key role in maintaining business continuity as flood prevention measures established to protect against prior events were easily re-deployed. The 2009 floods helped to demonstrate the value of those previous investments and get closer to the elusive ROI of BCM.

**Q What is the most critical element of a BC plan?**

**A** The most critical element of a BC plan is making sure the failover procedures are accurate and contacts up to date. This is accomplished by exercising it every year or more often as changes in technology or staff occur.

**Q When there's a natural disaster or outage, what is your role in the BCDR program and what do you do first?**

**A** We ensure company-wide coordination and communication via our Crisis Management Team as each impacted business unit utilizes their BC and/or DR plans to minimize the impact on employees and our customers.

## Technology considerations

**Q What role does technology play in managing risk and your BCDR program?**

**A** Technology has helped a great deal with minimizing and sometime eliminating risks. For example, today's call center platforms can manage customer call volumes and redirect calls to different centers when one office becomes overwhelmed. This technology can also be utilized should one site be impacted by a disaster. Similar technologies are available that provide uninterrupted access to data, applications, and websites even in the event that access to the primary servers is lost. Many of today's network technologies are designed to automatically re-route voice and data traffic when necessary to prevent disruptions.

**Q How have social networking and mobile technology influenced your crisis management role?**

**A** Mobile technology and social networking provide additional ways to communicate with employees and customers, which is critical for disseminating critical information during a disaster.

**Q What would you recommend to companies looking to invest in new BCDR technologies?**

**A** Companies of any size should look for technologies that provide cost-effective redundancies to help maintain business operations and provide a means to maintain communications with business-critical employees and customers.

**Contact your CenturyLink Representative today!**



## Evaluating BCDR plans and solutions

**Q How do you know you have good BCDR plans and solutions in place?**

**A** You need to look at business continuity as a program. If you build a plan and simply file it under business continuity until it's needed, you really don't know if it's a good plan. And you may not discover its weaknesses until disaster strikes and you are relying on the plan to keep the business up and running. The only way to validate a plan is to test it. You should test your BC plan frequently and strengthen it with the things you learn through testing.

**Q What trends should companies be watching?**

**A** Of course, there's a lot of buzz around Cloud-based services right now—and for good reason. Cloud-based services have the potential to change the way businesses use technology. They will allow businesses to rapidly deploy technology solutions as needed and then scale them down when not needed. That model is well aligned with the needs of a business continuity solution.

**Q What standards or certifications do you require your BCDR technology providers to have?**

**A** Several questions should be asked to evaluate a vendor's or supplier's program. First, do they have a program, and if so, can they tell me about it or provide a plan I can review? Do they have any certified staff managing the program? What events have impacted them in the past and how did they respond? I also ask if their program follows any particular standard to complete my view of their program.

### Important considerations for your BCDR plan

1. Know your priorities. If you don't focus (and plan accordingly) on what is most critical and prioritize, you're wasting your time.
2. Communicate. During a disaster, buildings are evacuated and people may scatter. It can be difficult to locate the people responsible for executing your BC or DR plans. 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 or social media to disseminate critical information if needed.
3. 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 the vendors and partners are that support your business. Consider your supply chain for daily business operations and have a back-up plan. Also, validate that your suppliers can do what they say they can do in case of a disaster.
4. 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's 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 the state agencies now to determine necessary credentials and processes to get people back into damaged areas quickly.

**Contact your CenturyLink Representative today!**



**Mike Cybyske**

Lead Disaster Preparedness Professional, CenturyLink

A certified business continuity professional with 15 years of BCDR experience, Mike Cybyske oversees the CenturyLink corporate crisis management team, which is responsible for minimizing or eliminating customer service disruptions. Mike leads more than 80 team members in continuous training, planning and readiness exercises to ensure coordinated response and recovery during disasters. As a CenturyLink crisis manager he also interacts with multiple local and state emergency management offices.

**Contact your CenturyLink Representative today!**

