

LESSONS FROM CATASTROPHIC EVENTS

5 KEY PLANNING GUIDELINES FOR DISASTER RECOVERY AND BUSINESS CONTINUITY

September 2017

Understanding the difference between Disaster Recovery and Business Continuity Planning

Disaster Recovery Planning and Business Continuity Planning are terms often used together or interchangeably, but what is the difference?

- Disaster Recovery Planning refers to how to recover your telecom and IT systems from disaster situations.
- Business Continuity Planning refers to how to plan for continuing your business in the event of a loss in local data connection or voice communications.

As more and more business is transacted over the Internet and more businesses leverage web or cloud-based applications, a primary concern is providing reliable and redundant Internet and secure data network connectivity. A local service outage affecting data or voice communications can lead to a major business disruption or disaster if unprepared.

While Disaster Recovery and Business Continuity Planning are different, both are equally important to ensure your business will survive unforeseen situations.



1

"For many small to mid-size businesses, a natural disaster or a ransomware attack could mean catastrophe. In fact, nearly 40 percent of small businesses never reopen after suffering a natural disaster."

Federal Emergency Management Agency

"75 percent of small businesses do not have a disaster plan in place. 52 percent say it would take at least three months to recover from a disaster."

Nationwide Mutual Insurance Co.

In This Report

- Building the Case for Business Continuity Planning
- Key Considerations
- Data Continuity
- Voice Continuity
- Leadership Examples
- Planning and Implementation
- 5 Key Planning Guidelines

Building the Case for Business Continuity Planning

Business Continuity and Disaster Recovery planning are very important for small businesses since they often lack the resources to cope easily in a crisis. Failure to plan could be disastrous. At best, you risk losing customers while you're getting your business back on its feet. At worst, your business may never recover and may ultimately cease operation.

In the event of a failure of voice or data services, consider what the cost per hour would be in lost sales or customer complaints if your customer service lines went down.

What is the cost in lost productivity if your employees cannot access the Internet or lose access to key corporate programs?

Here are some common beliefs of businesses who believe they are safe:

My staff all have cell phones which they can use for voice and data communications.

What is the cost in lost productivity if your employees have to inform customers and other business contacts that "We are experiencing a local service disruption. Please call my cellphone if you need to contact me." Extra time and resources would then be needed to advise customers when services are restored and regular contact numbers can be used.

What is the lost productivity in having employees use their cellphones to connect their laptops to the Internet?

Will they be able to access all their corporate files?

Would your data security be compromised if your employees had to communicate over the open Internet?

My voice services are already VoIP, so they are backed up.

Your voice services and voicemail may be in the cloud, but in the event of a data outage, how do you access them?

I have a managed data service so it is secure.

A managed service is supposed to provide monitoring but most often does not come with back-up redundancy.

Think Insurance

A data and voice continuity plan is like insurance. You need to ask yourself what is the cost in lost business and productivity in the event of a failure in voice or data communications for an hour, 4 hours or even 4 days.

For many major service providers, the mean time to repair a lost connection is four hours. You may be entitled to compensation of a small percentage of your monthly service fee. This is not likely enough to compensate for the business costs of the disruption.

You need to assess the potential costs of any disruption, how much redundant coverage you need and at what cost.

You can't predict the impact of a disaster, but you can plan for one. A carefully considered business continuity plan will make coping in a crisis feasible and enable you to minimize disruption to the business and its customers. In fact, it can also prove to customers that your business is robust and competent enough to cope with anything that disrupts business, possibly giving you the edge over your competitors.

Case in Point

A client had a 10 Mb managed fiber connection from a Tier 1 provider with a 20 Mb wireless back-up from an alternate provider.

One day, the IT department received a call from their data provider asking to confirm their data connection, as it was believed to be offline.

Sure enough the primary connection was down and had been for 4 ½ days, but no one at Head Office noticed as the failover to the back-up connection worked seamlessly.

Data Continuity

Service options and costs vary significantly from market to market.

Each key location for your business should have a secondary data connection both in case of emergency and to stream data applications such as Internet surfing or conference calls to alleviate usage on your primary data connection.

Ideally, the service will be from a different provider than your primary connection.

You need to evaluate how much bandwidth is required for your back-up. This is tradeoff between costs and benefits.

Where available, fixed wireless point-to-point is an excellent option. Local cable cuts can sometimes affect fiber, copper and cable services. Fixed wireless is generally stable enough to support Voice over IP.

Cellular can also be a good option with either a polled or flex data plan. In this case, you should use a commercial grade modem such as Oxygen or MicroHard rather than regular cellular hubs. As many computer control rooms are in a center or basement location, an external antenna or wiring from the cellular modem to the control room may be required.

Cable data service is also a good option. Again, you need to evaluate bandwidth requirements and costs. It has the added benefit of being able to offer TV coverage for the office or boardroom.

Once the back-up option has been identified, you will need to determine whether to program it for automatic or manual failover. If you have auto failover mode, then you should have access to bandwidth usage reports.

It has happened where a connection fails over to the secondary connection due to a slight glitch in the primary service and does not go back when the primary connection recovers. Businesses can unknowingly rely on the back-up connection without realizing it, until they get their next monthly invoice.

Voice Continuity - Legacy Phone Services

You should arrange to set up and enable the call forwarding feature with your telephone service provider.

For small and medium-sized businesses with a few lines in a hunt group, you should enable call forwarding on the main line to a designated cell phone number. Ideally, this cell phone will have voicemail to email provisioned, so that users can access voicemail without tying up the line. In the event of a voice service disruption, you would need to call the phone provider and activate the call forwarding. Your employees can use cellphones for outgoing calls to respond to messages.

For companies with a PRI, the call forwarding feature can be preset with the service provider to automatically activate in the event of a service failure.

For companies with multiple locations, calls can be forwarded to a direct number at a second location (preferably not in the same city), and the calls can be set to be routed back over IP to the phone system at the initial site. The phone system at both sites will need to be programmed accordingly. At the same time, the system at the failover site should have a voice mailbox set up for the incoming calls from the initial site. In the event of a regional failure, a back-up forwarding option to more remote sites should be set up as a contingency.

Voice Continuity – IP Phone Services

Business users of VoIP can expect a higher level of availability in the event of damage to their offices or to more general damage to a wider area. Your back-up voice channels are based on the redundancy and back-up of your primary VoIP provider. Much of the call routing in and out of your business is done by the SIP provider, who are typically in a different physical location. This means your SIP provider can reroute to another location when needed.

Assuming staff can find a location with Internet access, a laptop or smartphone may be enough to have them making and receiving calls. While no system is totally foolproof, one of the attractions of VoIP is its location flexibility.

In the event of a major system failure at your primary provider, then you could have a number set up (either cellular or with an alternate VoIP provider) to handle calls. In this case, you would likely need to inform employees and customers of this back-up number.

Leadership Examples

For leadership and decision-making in a crisis situation, consider these examples:

[Remote Working](#)

The offices of PCPC Direct, a Houston-based solution provider, enacted their business continuity plan during Hurricane Harvey. Even though PCPC Direct offices were high and dry, surrounding areas were inundated by floodwaters. Email, applications and terminal services were already established for off-site employees, so this allowed accounting, administrative and help desk teams to work remotely.

Beyond the inconvenience of working remotely, PCPC services remained largely uninterrupted. Customers that rely on PCPC for hosting and data protection have been running on its platform soon after Harvey passed through.

[Failover Data Center](#)

Computex Technology Solutions, a national cloud and managed services provider has their Houston data center 10 feet off the ground to eliminate the threat of rising waters.

Computex also has a failover data center in Minneapolis it tested in June in preparation for the hurricane season. This arrangement allows services to be shifted to Minneapolis when necessary and customer data would be protected.

If any of Computex customers lose power inside their own facilities during a storm, Computex opens their doors for them to walk in, plug in, and work. During Hurricane Ike in 2008, over 250 Computex customers were able to continue to work in Computex offices.

Planning and Implementation

Once your Business Continuity Plan has been implemented with back-up data and voice connections, it should be tested outside regular office hours. The plan should be clearly documented so the IT department and key employees know what to expect and how the back-up is to be implemented.

Some major providers will offer services for both voice and data back-up. However, it is not the preferred solution to use the same provider for primary and back-up. In the event of a major outage, they may be too busy to provide assistance.

While these are basic guidelines to help you explore and prepare, there is more to do. Rather than simply waiting for disaster to strike, the most reliable businesses are putting strategies in place to handle disruptive events with greater efficiency. It may be beneficial to use data or communications consultants to identify the requirements, budget and options for your Business Continuity plan.

5 Key Planning Guidelines

When it comes to business and disaster recovery, being prepared for potential disasters is key. Here is our Disaster and Business Recovery Checklist with 5 key planning guidelines:

1. Assess the problem and its impact

Before doing anything, understand the underlying issue and how it will impact your customers. Is the issue local to one machine, or does it affect your entire system? Have files been deleted or are servers / workstations down?

2. Establish recovery goals

Plan out your road to recovery.

- Identify critical systems and prioritize recovery tasks
- Restore the system, the data, or both?
- What date/time should you recover from?

3. Verify the recovery and confirm functionality

Once a recovery is verified, confirm that it interacts positively with users.

- Test network connectivity.
- Ensure all users can access resources and applications in the recovered environment.

4. Restore the original systems

Decide which restoration process will work best. i.e. virtual machine, bare metal

5. Self-assess afterwards

After it's all said and done, take a step back and think about it: How well did your team do? What could you have done differently?

- What precipitated the failure?
- What ongoing issues need to addressed?
- What can be done better in future disaster scenarios?

What Catastrophic Events Teach Us about the Need for Disaster Recovery

Hurricane Harvey, one of the most destructive storms in the history of the United States, made landfall in southeast Texas on August 25, 2017. The storm brought torrential rain which led to catastrophic flooding and displaced thousands of people. The following week, Hurricane Irma's path of destruction spread throughout the Caribbean and the south coast of Florida.

After events like Hurricane Harvey and Hurricane Irma, a large percentage of businesses will never fully recover or will be forced to close permanently.

Why Businesses Need Disaster Recovery Plans Now

Disaster recovery is critical for any business that relies on technology. Hurricanes Harvey and Irma highlight an important lesson for businesses. Companies that rely on technology to store and transfer data and to operate their businesses need to be prepared for the possibility that a disaster could occur at any time. Failing to prepare could leave a business crippled.

A third-party technology agnostic consultant can help you create a disaster recovery and business continuity plan so you can get back up and running as quickly as possible after a disaster. As we have learned, and some the hard way, it's better to be safe than sorry.



About Us

Abilita is a Communications Technology company whose experts provide independent and technology agnostic consulting solutions to a diverse set of SMB to enterprise organizations. With locations across North America, Abilita offers advice on and implementation of business continuity that our clients have come to rely on equally during normal business periods and throughout catastrophic disruption.

For our report [8 Steps to Planning your Emergency and Disaster Plan](#), or more information about telecom or your custom technology needs, go to www.abilita.com or call 1-800-836-4968.