Business Continuity Planning Essentials
SORRY
we're closed
Data is essential for all types of organisations today, so ensuring access to mission critical applications and data following a disaster is crucial. However, business continuity and disaster preparedness are about so much more than that.

The first step for many businesses is to conduct a business impact analysis:

- **Identify potential events that could negatively impact normal business operations.**
- **Calculate the likelihood that each event may occur.**
- **Quantify the impact that the event could have on your business.**

There are a wide variety of threats to any business ranging from natural disasters to security breaches to random accidents. So, crafting specific plans for risk mitigation, disaster response and continuity of operations is essential.
Ensure Employee Wellbeing

The specifics will vary widely from company to company, but your emergency safety and communication plan must address the following:

• How the company will ensure employees are safe during a disaster event.

• How it will communicate essential information to employees following the event.

Effective Communication

E-mail is the easiest way to reach a large group of employees, but if your company's email server is down, you are out of luck. Some businesses employ redundant Exchange servers or cloud-based services to ensure email access. Of course, if you are without Internet access entirely, you'll need an alternative. It is essential to test and update the communications plan periodically.
If an event occurs that is likely to impact your customers, it is essential to communicate the details of the issue and explain the steps you are taking to mitigate it. This might mean direct communication to your customers, but it could also mean messaging via traditional and social media. Your organisations ability to respond to customer needs following an event will have a direct impact on reputation.

So, how do you keep your good reputation intact?
It comes down to preparation. Carefully planning communications with customers is essential.
You also need to ensure access to communication infrastructure (phone, email, Internet access).
Testing is the best way to identify and resolve customer support weaknesses and communication infrastructure issues.
Enable IT Uptime

It really wasn’t very long ago that backup meant daily incremental and weekly full backups to tape or a dedicated disk backup target. Duplicate tape copies were created and shipped offsite for disaster recovery, typically to a secondary site maintained by the business or to a tape vaulting facility. Many businesses continue to use this model today and, depending on your recovery needs, it may be perfectly adequate. However, disaster recovery from offsite tape can be slow and this, of course, means considerable downtime.

When creating an IT disaster recovery plan, it’s important to understand two concepts: recovery time objective (RTO) and recovery point objective (RPO).

RTO is the amount of time that it takes to get a system restored following a failure or disaster event.

RPO is the point in time to which data can be restored following the event.

Recovery In-Place & DRaaS

Today, users can run applications from image-based backups of virtual machines.

This capability is commonly referred to as “recovery-in-place” or “instant recovery.” Recovery-in-place technology allows you to run applications from the onsite appliance or from the cloud following an outage or disaster. This is commonly referred to as “cloud disaster recovery” or “disaster recovery as a service” (DRaaS).
Keep Business Moving

If your employees or customers do not have access to essential applications and data, there will be a direct impact on productivity and revenue. While this sounds obvious, many organisations do not consider the actual costs of downtime for a business.

Continuity of Operations

Application downtime is, of course, just one factor that can impact your bottom line. Again, there are a broad spectrum of possible considerations depending on the size and type of your organisation. However, there are a variety of examples that apply to many businesses.
Insurance

It is essential to select the proper insurance coverage for your business' specific needs. It is also critical to document all insurance information.

Training

Every business will need to identify employees critical to the recovery process. Whatever the structure of your business, you will need to define business continuity roles and responsibilities.

Facilities

It is critical to evaluate the facility or facilities in which your business operates.

Considerations might include but are not limited to:
* Appropriate fire suppression systems
* Generators capable of powering essential equipment
* Uninterruptible power supply systems for critical servers
* Surge protection systems
* Alarm/intercom systems to alert employees of emergencies

Dependancies

It is important to consider dependencies within and especially outside of your organisation.
To Sum Up

Disaster recovery and business continuity planning should be considered a critical aspect of running a business. However, many organizations disregard it completely. Others have a plan in place, but fail to grasp how time consuming the recovery process can be and the associated cost of downtime. The good news is that today’s data protection technologies and services have greatly improved the IT piece of the business continuity puzzle.

Ask us anything

@PCSbusiness

www.pcs-systems.com