Top 10 Business Continuity Plan Must-Haves

kinetic business by windstream

Disasters can take many shapes. Extreme weather, fires, malicious attacks, even a power outage or staff disruption due to illness or work stoppage can wreak havoc on a business's reputation and bottom line. Across all industries, there is less tolerance than ever for any kind of downtime, and more than half (58%) of small to midsized businesses are unprepared for data loss.[1] So, plan now. Understand that while business continuity covers every aspect of your operations, your network and other IT functions should be at the top of your list.

When developing your business continuity plan, be sure to incorporate these top 10 key communications and technology items:

1. Compile an inventory of hardware such as servers, desktops, laptops and wireless devices, as well as software applications and data. Analyze applications to determine how big of a role they play in generating revenue.

2. Your data, critical applications and networks should be, at a minimum, continuously backed up and mirrored in the cloud. This will ensure that all your electronic records and invoices are safe and available, even in the event of a disaster.

3. Identify critical software applications and data and the hardware required to run them. Ensure that copies of program software are available to enable reinstallation on replacement equipment. Establish a hierarchy of hardware and software restorations.

4. Prioritize company functions in the immediate effort to keep your business running and your employees productive. In a short-term emergency, not every single function can be replicated, nor should it be.

5. Determine Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) based on your business's threshold for data loss and downtime. RPO is the maximum tolerable period in which data might be lost from an IT service due to a major incident. RTO is the duration of time and a service level within which a business process must be restored after a disruption in order to avoid unacceptable consequences associated with a break in business continuity.

6. Partner with an Internet provider that offers automatic failover to a wireless Internet backup connection in the event of a primary Internet service disruption. Specifically, look for one that offers 24/7 dedicated business support and a 99.999% Internet Uptime SLA (service level agreement).

7. Be sure to adhere to the rules or regulations governing your industry, which may dictate certain aspects of your IT disaster recovery plan. If you had a business failure, would you be able to maintain compliance with regulations such as Sarbanes-Oxley, HIPAA, PCI-DSS, etc.?

8. Consider implementing cloud solutions for voice communications, as doing so will ensure open lines of communication among employees, customers, partners and vendors in the event of an emergency.

9. Execute security risk assessments around specific data security threats such as virus protection, intrusion detection, hacker prevention, network events, component failures and systems crashes.

10. Perform recovery tests and assess how quickly and accurately your business and technology were restored. Use the results to improve your plan and continue to perform regular tests, because a plan is only good if it can be successfully implemented.

[1]https://smallbiztrends.com/2017/04/not-prepared-for-data-loss.html

026723 01/20

kinetic business by windstream