YOUR GUIDE TO
BUSINESS CONTINUITY & DISASTER RECOVERY

According to statistics uncovered by researchers such as the US Small Business Administration, SMBs who are unable to reopen within five days after a disaster fall into the category of, **nine out of ten of those businesses will fail within the following year.** Despite the high risks and costs associated with unplanned downtime, many SMBs are struggling with disaster readiness and are **underprepared** for significant business disruptions.

To reduce threats to your mission-critical applications and resume operations as quickly as possible, your business should be equipped with an exercised business continuity and disaster recovery plan before you take the hit.

Assess your business continuity and disaster recovery plan to determine if you will meet your recovery time objective (RTO). Your RTO is how much time you have to restore your processes after a disaster to avoid business breaking consequences.

DOES YOUR PLAN IDENTIFY THE IMPACTS OF:

- Lost sales and revenue
- Loss of customers

DO YOU KNOW WHAT IS THE MINIMUM ACCEPTABLE PRODUCTION OR SERVICE LEVEL TO AVOID?

Your RTO should be assessed to guard against this level, so it doesn't generate negative impacts on:

- Customer requirements
- Deadlines
- Hold back during peak business seasons

Need help building out your Business Continuity & Disaster Recovery plan and quantifying your RTO?
We are here to help. ***Contact us today to discuss your needs and establish the right solution for your business.***

Professional Telecommunications services, Inc. www.ptscinti.com | Cincinnati OH | 513-232-7700 | 800-365-1085

CYBER THREAT RECOVERY & REMEDIATION

Coupled with your Business Continuity & Disaster Recovery plan, you will want to incorporate these application needs to help reduce your organizational risk exposure to allow for quick remediation:

ENDPOINT SECURITY

This will help you determine what events took place and when to aid in isolating malware and stopping further spread

DNS SECURITY

You will want to make sure your solution is able capable of turning away security threats at the network level

ENDPOINT BACKUP/RECOVERY

Select one that will safeguard your data should the DNS and/or endpoint security solutions be compromised

RECOVERING YOUR DATA IS ESSENTIAL, BUT YOU WILL ALSO NEED TO DEVELOP A ROBUST REMEDIATION PROCESS TO PREVENT FURTHER INFECTION OF SYSTEMS AND PROLIFERATION OF MALWARE.

You will want your team to be ready to act quickly, with key steps that include:

- Once detected, suspend all devices or compromised devices at a minimum.
  Block traffic from the infected areas if network segmentation is enabled to help block spread.
- If backups are still running, they should also be suspended to stop infected data from being backed up.
  This can be done from a dashboard or automated scripts and APIs.
- Understanding how malware entered your network is critical to fend off future breaches.
  You will want to verify the discovery date, dwell time, and when the malware started executing.
- Figuring out the timeline of events will prove to be critical to your recovery and restoration process, particularly so you can set your restore time.

The right tools, planning, importance hierarchy, and communication channels across your business are essential for establishing resilience in an increasingly cyber world.

We can help you put a plan in place or support your business by managing the recovery and remediation for you. *Contact us today to learn more!*

Professional Telecommunications services, Inc. www.ptscinti.com | Cincinnati OH | 513-232-7700 | 800-365-1085