HURRICANE PREPAREDNESS GUIDE FOR BUSINESSES

AN INFORMATION TECHNOLOGY PLAN

www.TechRageIT.com

TECH RAGE IT

If your business doesn't have a Disaster Recovery Plan or hasn't tested it in years, here are 5 cold hard facts to consider:

1. Over half of the small businesses in the U.S. have experienced disruptions in day-to-day business operations. 81% of these incidents have led to downtime that has lasted anywhere from one to three days.
2. $5,600 is the average cost of downtime per minute.
3. 80% of businesses that have experienced a major disaster are out of business within three years.
4. Disaster recovery solution providers estimate that 60% to 70% of all business disruptions originate internally – most likely due to hardware or software failure or human error.
5. 34% of SMBs never test their backup and recovery solutions – of those who do, over 75% found holes and failures in their strategies.

Hurricanes have the potential to cause massive destruction. That's why developing a plan well in advance provides much-needed peace of mind. This guide provides suggestions to help your organization prepare for a hurricane's effect on your business' operations, technology, and employees.

1. Have a Disaster Recovery Plan in Place

- Identify the current status of your existing Disaster Recovery Plan (DRP). Do you have one and when was the last time you tested the plan?
- Determine the vulnerability of your business' technology infrastructure (servers, switches, etc.) to natural disasters, including tornadoes, floods, and fires.
- Determine which systems or data must be recovered in minutes, hours, or days to get your business back to running efficiently.
- Establish the need for off-site data backups and storage for critical data.
- If your backup site is within the area that may be affected by a storm, consider backing up to a more remote site or the cloud.
- Create a technology plan that includes hardware, software, facilities, and service vendors.
- Review the plan with vendors. Secure from them a clear understanding, and commitment of the plan.

TECH RAGE IT

- Perform risk assessments around specific threats and implement data security management such as anti-virus software, intrusion detection system, hacking prevention, network events, component failure accidents, and systems crashes.

- Review prior recovery events, if applicable, to determine how quickly and accurately your business and technology were restored. Apply any lessons learned so they can be addressed in future planning.

- Determine the effectiveness of your data backup and recovery policies and procedures. Are the procedures fully documented and accessible to key management and staff?

- Perform a dry run, or a practice exercise, to uncover and fix potential problems before going live.

- Test remote access to your servers and email systems.

- Prepare an incident response plan for mitigating a security breach. Review the plan annually, as security threats can change.

2. Prepare Your Organization and Vendors

- Have an emergency communication plan in place before the storm, evacuation, or threat to begin advance notifications.

- Identify your key audience (stakeholders, staff and remote workers), that needs to be contacted and updated with critical information. Build and maintain accurate employee distribution lists.

- Identify alternate employees who can carry out tasks in the event key staff members cannot be reached.

- If you need to close all threatened office locations, consider the essential resources your key remote workforce may need to continue business operations: power generators, portable charging stations, mobile WiFi hotspots, and phone landlines (in the event of mobile phone outages).

- Internet providers may activate free public WiFi hotspots to stay connected after a storm. Create documentation that explains how to access those networks through devices. However, cyber security training, such as using VPN, should be provided regularly to reduce risks.

- Identify potential co-working or off-site locations to perform essential tasks. Plan for closed roads, communications, data connectivity, desktops or laptops and workspace at those sites.

- Discuss the plan with your building management so they have a clear understanding of their role in safely securing the building and your employees. Obtain 24-hour security if needed.

- Reach out to third party partners and ensure they also have a documented plan in place that meets your needs. Review periodically to keep the plan current.

- Review your insurance policies to mitigate any possible gaps in coverage.

3. Before, During and, After a Hurricane

Before the Hurricane

- Identify your key staff members, remote workers and/or team with defined roles for preparedness and response planning.
- Have contact information for all employees, vendors, and clients on hand.
- Back up all data on servers and personal computers. Be sure they are accessible from anywhere.
- Shutdown all computers and printers at close of business. Confirm which equipment must remain connected to a power source. Check the integrity of any uninterruptible power supplies (UPS).
- Unplug Ethernet cables from back of computers, docking stations, phones, faxes and printers; unplug monitors and other computer peripherals from the wall outlet or surge protector.
- Place all computers and other technology on top of desks or other high and dry locations, away from windows and doors. Determine if laptops should be taken home or placed in a secure location.
- Cover equipment with plastic sheeting if building is prone to leaks. DO NOT cover equipment that is plugged in or powered on.
- Redirect business phones to a softphone application to make VoIP calls directly over computers, tablets or smartphones.

During the Hurricane

- Monitor any equipment that must remain connected to a power source.
- Continue to communicate with all key audiences until the strom has passed.

After the Hurricane

- Wait until the location or affected area is declared safe before traveling to and entering the site.
- Take note of the condition of the computer equipment. If it is visibly damaged or appears to be wet, do not plug the equipment in or turn it on.
- Computer equipment should not be turned on if electrical power is unstable.
- Central services such as network connectivity, network file servers, or email servers may not be available immediately when power is restored.
- Return the computers to their original locations and reattach all peripherals. Plug in all power cords/Ethernet cables as they were before, and turn the computer on. Take note of error messages.

If you need help with Disaster Recovery Planning, contact us today!
Hurricane season starts June 1st.

TECH RAGE IT