HURRICANE IT CHECKLIST

CRESCENT
IT SYSTEMS

With Houston vulnerable to tropical storms and hurricanes, it is important to understand your risk, develop a preparedness and mitigation plan, and to take action. It will not only increase the safety of your employees and clients, but will help keep you in business after a disaster.

FEMA and the Department of Labor stated that over 75% of businesses without a business continuity plan will fail after a natural disaster.

This checklist will help take action to protect employees, clients and help plan for business continuity.

1 Identify what is most important

COMPLETE - DEVELOPING - LACKING

1. Assess your location(s) ability to withstand flooding, power outages, wind and risky environmental conditions. Identify what fortification steps could be made to protect the location, external & internal business assets and staff. Identify what level of environmental threat would signal an evacuation of the location(s) and ceasing of onsite operations. □ □ □

2. Identify key employees and the team with specific roles and knowledge of the business operations to coordinate the planning and identification of actions to be taken during a disaster. This will include steps to be taken to cease and migrate operations to a recovery site and to define the methods of communciation to be used. □ □ □

3. Perform a business process and operations analysis to determine which are the critical processes need to be recovered first, and at what level to sustain the business. Identify what essential resources & time that are needed to provide the services or products, including staff, materials, tools, technology and vendors, and how to restore them. □ □ □

4. Quantify what are the potential costs of a disruption or downtime from a disaster and create a budget depending on the various possible threats that have been identified. □ □ □

5. Perform a general inventory of the essential technology assets needed to conduct business and all aspects of their management and configuration. □ □ □

6. Identify how and to where the identified critical assets needed for business can be migrated. Determine the transportation, time and personnel needed to transport and reassemble the assets. Cost of personnel and the transportation of the assets must be assessed. □ □ □

Want to know more? We can help!

HURRICANE IT CHECKLIST

IT Recovery strategies should be developed for Information Technology (IT) systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity. Priorities and timeframes for IT recovery should be consistent with the priorities for recovery of the business functions and processes that were developed during the business impact analysis.

Information Technology systems require hardware, software, data and connectivity. Without one component of the "*system*", the system may not run. Recovery strategies should be developed to anticipate the loss of one or more of the following system components: power, internet connectivity, data, software applications, computer room environment with backup power and AC.

2 Developing IT Disaster Recovery Plan

	COMPLETE	DEVELOPING	LACKING
7. Do you have a existing disaster recovery plan that has been tested?	□	□	□
8. Compile an inventory of hardware (e.g. servers, desktops, laptops and wireless devices), software applications and data. Identify critical software applications and data and the hardware required to run them.	□	□	□
9. Identify data on network servers, desktop computers, laptop computers and wireless devices that needs to be backed up along with other hard copy records and information. Lost or corrupted data can lead to significant loss.	□	□	□
10. Is the data being backed up daily and a local backup copy being stored offsite? Data should be backed up as frequently as necessary to ensure that, if data is lost, it is not unacceptable to the business.	□	□	□
11. Is a cloud backup being utilized? Most use a cloud backup solution in addition to a local copy, ensuring there is a reliable and timely offsite backup.	□	□	□
12. IT resources required to support time-sensitive business functions should be identified. The recovery time for an IT resource should match the recovery time objective for the business function that depends on the IT resource.	□	□	□
13. Review the existing IT migration plan or create a plan that details how the company can operate if the current IT resources are unavailable. All elements that enable the critical IT resources to run will need to be identified.	□	□	□
14. Is there an alternate site of where the data operations can be migrated to? Are there duplicate resources already established offsite to serve as a recovery site? Crescent IT Systems can assist in identifying solutions to migrate IT operations for companies.	□	□	□
15. Have you assessed your data security in regards to virus protection, network security, data backup media, and hacker prevention and have a mitigation plan.	□	□	□

HURRICANE IT CHECKLIST

CRESCENT
IT SYSTEMS

At this stage, critical business functions, processes, costs and supporting resources have been identified, along with a risk assessment of the location(s) and an IT Disaster Recovery Plan steps have been identifed and documented along with IT asset migration plan.

The next steps involve communication and education of your employees of their roles and communicating with your vendors to ensure supplies and services are not disrupted. Fortification steps for the location(s) are planned and expectations are set.

3 Fortification, communication and education

COMPLETE - DEVELOPING - LACKING

16. The Business Continuity Plan must be finalized and signed off by top management to ensure buy-in from the top management prior to rolling out the final employee roles and expectations. □ □ □

17. Using the information learned in the risk assessment in step #1, form the resource and implementation plans to deploy the fortification of the location(s), both the interior and exterior of the buildings. □ □ □

18. The roles and functions for the employees who are critical for the operations of the business as well as those coordinating the migration of the business functions during a threat, are to be trained and expectations set. The methods of communciations discussed earlier for disaster recovery activites are decided upon and published. □ □ □

19. The vendors that provide services and supplies to your business should be vetted for their ability to provide during a disaster. Agreements for their service must be reviewed and in place. Communication methods to be used with these vendors must be agreed upon. □ □ □

4 Final test and validation

COMPLETE - DEVELOPING - LACKING

20. A plan is not finished until it is tested. A simulated threat should be used to test the reaction and recovery of your business operations and Business Continuity Plan. A annual review of the Business Continuity Plan should be performed to ensure that changing business elements are accounted for within the plan. □ □ □

Hurricanes may happen during June to November each year but storms and other disasters can happen all year long. Businesses need to prepare for the disruptions and downtime that the weather can cause to their business. If you have questions, we can help!

Call today to start protecting against disasters!

www.crescent-systems.com - (281) 358-3589
pegarrison@crescent-systems.com * 9600 Long Point Rd., Suite 228, Houston TX 77055