



Top 10 Actions A CIO Can Take To Prepare For A Hurricane

Practical advice from well prepared CIOs of
Gulf Coast companies

Overview

While the 2007 hurricane season was very active with 15 named storms of which 2 were major hurricanes, costing \$7.5 billion and 416 lives, the predictions for the 2008 season appear to be very similar. And, no one can forget 2005's Hurricane Katrina that cost over \$120 billion in damages and over 1,800 of lives.¹

Active hurricane seasons like these impose an unwelcome set of challenges for CIOs. Immediate concerns include the safety and security of employees as well as the prevention of damage to physical facilities. However, CIOs must also address the challenge of maintaining business continuity. Short and long-term impacts on customers, suppliers, partners, and employees can arise if communications and critical IT systems are lost for even a short period of time.

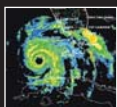
In the days and months following the devastating hurricanes that struck Florida and New Orleans in 2005, a handful of businesses fared much better than average. These companies had the right programs in place, they executed strategies with built-in flexibility to swiftly react to changing situations, and ultimately provided excellent resilience for their organizations. While most companies struggled for months to bring their operations and staff back to capacity, these select organizations remained open for business, quickly relocated staff, and were able to recover without a devastating financial hit.

What sets these companies apart from the rest? They are not necessarily the largest, wealthiest or most influential companies in their regions: in fact some organizations that fared well through the hurricanes are very small – they merely had a well-executed plan and the right set of tools.

¹NOAA.

01

Make sure you can communicate instructions to employees no matter what happens to the prevailing communications infrastructure

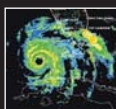


"If you can't communicate, you can't recover."

These are the first words of advice heard from companies that have been through a disaster. You cannot predict which systems will be affected by a hurricane, or what your staff will have access to at any given time. Each storm may have a different and unpredictable effect on infrastructure. For example, following Katrina, BlackBerry® was the only network that was available; however, POTS phone service continued to work throughout most of the Florida hurricanes of 2004. Many crisis communications systems take advantage of a limited number of communications channels. Ensure your system enables multiple communication channels with flexible and custom escalation paths to devices that your staff may have access to.

02

Collect and maintain up-to-date contact information for your employees and key constituents



If you do have a crisis communications system in place, it will be ineffective if you do not have the correct contact information for your recipients.

Your HR system, email system and distribution lists, or other system of record for your employees' contact information can be used as the system of record of current contact information – and may be synchronized with any crisis communication system you implement. Develop a process that is required to collect your staff's preferred method of contact, and **make sure you have several channels to reach each employee.**

03

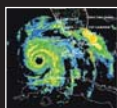
Plan for your post-storm roll call of employees



A broadcast set of emergency instructions with no feedback or visibility into the recipient status only does half the job of a true crisis communications infrastructure. Implement a system that enables a roll call and 2-way communications, so you can locate all employees and identify any that need help.

04

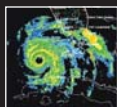
Plan for a remote recovery facility



In case your physical facilities are incapacitated for a long period of time, plan to move to a workspace with access to critical business systems. Ensure your company's work product documentation is securely archived and accessible from a remote location. Plan with the assumption that your internal local infrastructure will not be available.

05

If you can protect one application, protect your email – you will need it



Email often provides the status of work in progress and is the preferred medium for most employee communications. Email access is usually required to continue to function smoothly or to recover in times of crisis. Ensure your organization has comprehensive email protection regardless of what happens to your local infrastructure.

06

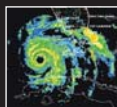
Have a system in place to avoid losing compliance and audit trails when there is a crisis



For example, if your employees use an alternate email system such as their personal email accounts to conduct business during or following a storm, all of these messages may be unrecoverable to your primary system. Have an email continuity system in place so employees have no need to use alternate email systems. Keep archiving all of your business transactions to help ensure there will be no breaks in an audit trail.

07

Complete a DR audit of your vendors, especially local vendors

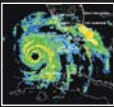


If your website is hosted locally, it is likely to go down during a storm. Consider hosting some of your key services in other geographies.

Understand the business continuity and disaster recovery plans of each of your key vendors, and plan ahead a method of communicating with them in the event of a crisis.

08

Complete a surprise off-hours test of your emergency plan



Practice executing your emergency planning with some of your key staff members **out** of the loop. Ensure “backup” staff members are able to administer an emergency plan, send out a notification, perform a roll-call, etc. Verify that you can reach key staff members through multiple channels (cell phones, pagers, home phones, remote office phones). Test that your emergency communications system can escalate action items if key members can’t be contacted within a prescribed amount of time.

09

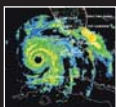
Plan to *not* stick to your emergency plan



You need to have a plan that is executable; however, in real situations, circumstances can change so rapidly and in unpredictable ways that you need to make ad-hoc decisions and execute on them. Your company's leadership needs the ability to change instructions rapidly and to notify employees with up to the minute information. Everyone who has managed their business through a major storm has a common experience: Nothing goes exactly according to plan and you must have the ability to change plans "on the fly."

10

Identify key operations and their recovery priority



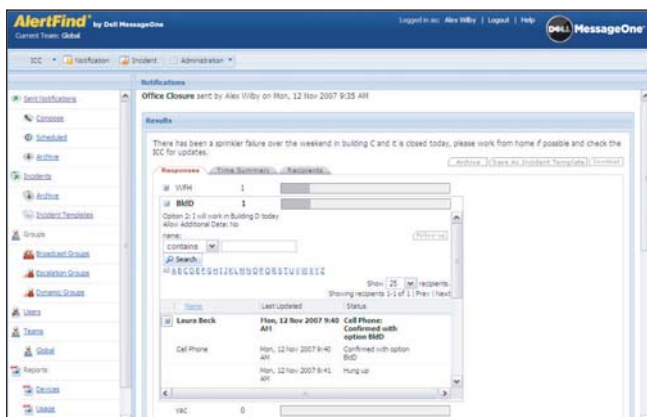
While conditions may dictate the availability of business operations, the overall business impact of operations and processes can be established before the storm. Prioritize and publish recovery sequence plans to minimize the outage effects on the business, customers, suppliers and employees.

Crisis Communications and Collaboration

During and after a hurricane, normal lines of communication often fail when you need them most. Reaching employees and their leadership teams located in unusual sites is a challenge that most companies cannot meet. That's why many leading organizations, communities, and schools, depend on Dell MessageOne AlertFind. AlertFind's crisis notification service harnesses all available commercial communication channels to help find people, deliver messages, and collect information. AlertFind's Incident Collaboration Center offers additional collaboration tools to manage through crisis events and accelerate recovery times.

AlertFind is designed from the ground up to meet the unique needs of large enterprises for multi-team support, security, data integration, compliance auditing, and mass notification to thousands of users in minutes.

- Automated message delivery and escalation
- In-bound communication lines for hard-to-reach contacts
- Enterprise data security and access control
- Real-time auditing and reporting
- Full global support
- Web services Application Protocol Interface (API) for integration with corporate systems
- Collaborative incident logs to track events
- Formal task management and secure document sharing
- Publicly share information via emergency website



Dell MessageOne™

Email Management Services™ – Continuity, Archiving, and Security

In addition to communicating with employees, email must continue to function to allow continued business operations. The Dell MessageOne Email Management Services (EMS™) is capable of providing comprehensive email protection in a single, on-demand service.

EMS helps eliminate the downtime, compliance, and financial risk of managing email. Deployed in a day, affordably priced, and requiring minimal maintenance, EMS' integrated continuity, archiving, and security services helps lower costs and maintenance complexity.

- Help eliminate email downtime and data loss
- Make email outages virtually invisible to users
- Control retention, accelerate e-Discovery
- Globally search archives in seconds
- Reduce data stores as much as 80%
- Effectively filter spam and viruses
- Achieve a low TCO for a very high level of protection

EMS provides the control and flexibility to meet evolving email challenges, EMS can effectively eliminate the risks of managing email.



For more information please visit www.messageone.com



www.messageone.com
1-888-367-0777

Dell MessageOne
11044 Research Blvd.
Building C, Fifth Floor,
Austin, TX 78759

V0708