



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

“Practical advice from the best-prepared CIO’s of
Gulf Coast companies”

Overview

While the 2006 Atlantic Hurricane season was relatively benign, 2005 was a season of records: With 28 named storms, a record four hitting the U.S., over \$100 billion in economic damage and the loss of over 2,200 lives. Hurricane Katrina alone accounted for over \$40 billion in economic damages. And, 2004 brought its own onslaught of devastating storms to Florida.

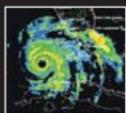
Storms like these impose an unwelcome set of challenges for CIOs. Immediate concerns include the safety and security of employees as well as the prevention of damage to physical facilities. However, CIO's must also address the challenge of maintaining business continuity. Short and long-term impacts 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, 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.

01

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



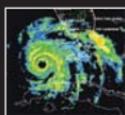
"If you can't communicate, you can't recover."

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

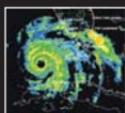


If you do have a crisis communications system in place, it will be ineffective if you do not have the correct contact information for your recipients.

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

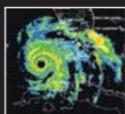
Plan for your post-storm roll call of employees



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

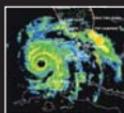
Plan for a remote recovery facility



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

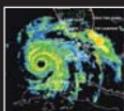
If you can protect one application, protect your email – you will need it



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

06

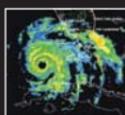
Have a system in place that does not lose compliance and audit trails when there is a crisis



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 will be out of compliance and unrecoverable to your primary system. Keep archiving all of your business transactions and ensure there will be no breaks in an audit trail.

07

Complete a DR audit of your vendors, especially local vendors

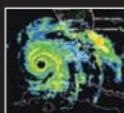


If your website is hosted locally, it is likely to go down during a storm. Consider hosting some of your key services in other geographies.

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

08

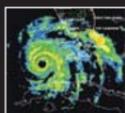
Complete a surprise off-hours test of your emergency plan



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

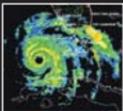
Plan to *not* stick to your emergency plan



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 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.

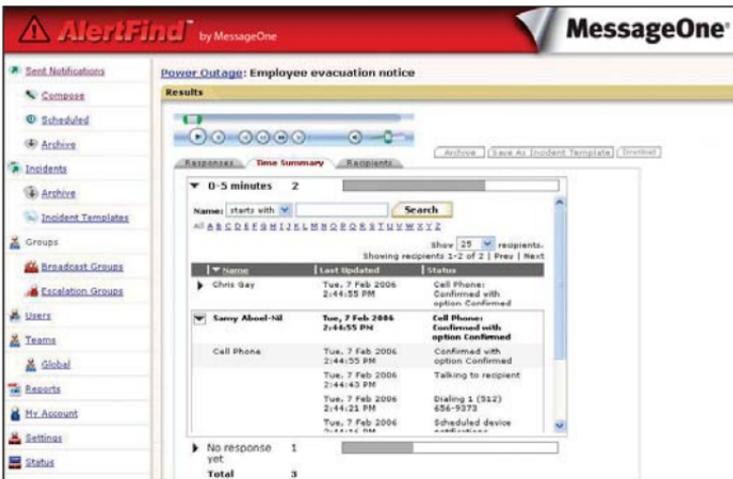
MessageOne

AlertFind® – Automated Crisis Communications

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 currently meet. That's why leading organizations, communities, and schools, depend on MessageOne's **AlertFind** for an immediate, direct two-way communication channel during emergencies and disasters.

Unlike email or manual call-trees, AlertFind provides executive leaders with the ability to communicate, instruct, and manage in real-time during a crisis. AlertFind provides the most effective method to quickly, securely, and reliably distribute and collect information using all methods of communication. By leveraging email, voice calls, text messages, pagers, and other communication channels, AlertFind provides an automated method to find people, deliver messages, and gather information in real-time.

MessageOne's AlerFind



MessageOne

EMS™ – Email Continuity, Recovery, Archiving, and Security

In addition to communicating with employees, email must continue to function to allow continued business operations. MessageOne's **Email Management Services (EMS)** is the first and only solution capable of providing total email protection in a single, simple service.

EMS eliminates email downtime and data loss in the primary environment while delivering the many benefits of email archiving with a back-up email system:

- Total protection for users from email downtime
- The complete elimination of data loss
- Worry free retention policy management
- Instant eDiscovery for email and attachments
- Significantly reduced storage costs yet increased user mailbox sizes
- The most cost efficient architecture to achieve total email protection

As a managed service that fully integrates with Active Directory® and Microsoft® Outlook®, EMS eliminates downtime, eliminates the risk of data loss, reduces cost, and shrinks maintenance, backup, and recovery times. EMS has been the choice of over a thousand companies and can be deployed in as little as one day.

MessageOne's EMS

The screenshot shows the MessageOne EMS Administration Console. The interface includes a navigation menu on the left with options like 'Admin Console Home', 'ActiveMailbox', 'User Administration', 'BlackBerry Administration', 'Mailboxes and Aliases', 'Mailing Lists', 'Notification Status', 'Audit Reports', and 'Your Account'. The main content area is divided into several sections: 'Readiness Check' with status indicators for various services; 'User Statistics' showing mailbox synchronization; 'Current EMS State' with a 'Start Recovery' button; and 'Current Tests'.

For more information please visit www.MessageOne.com

MessageOne®

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

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