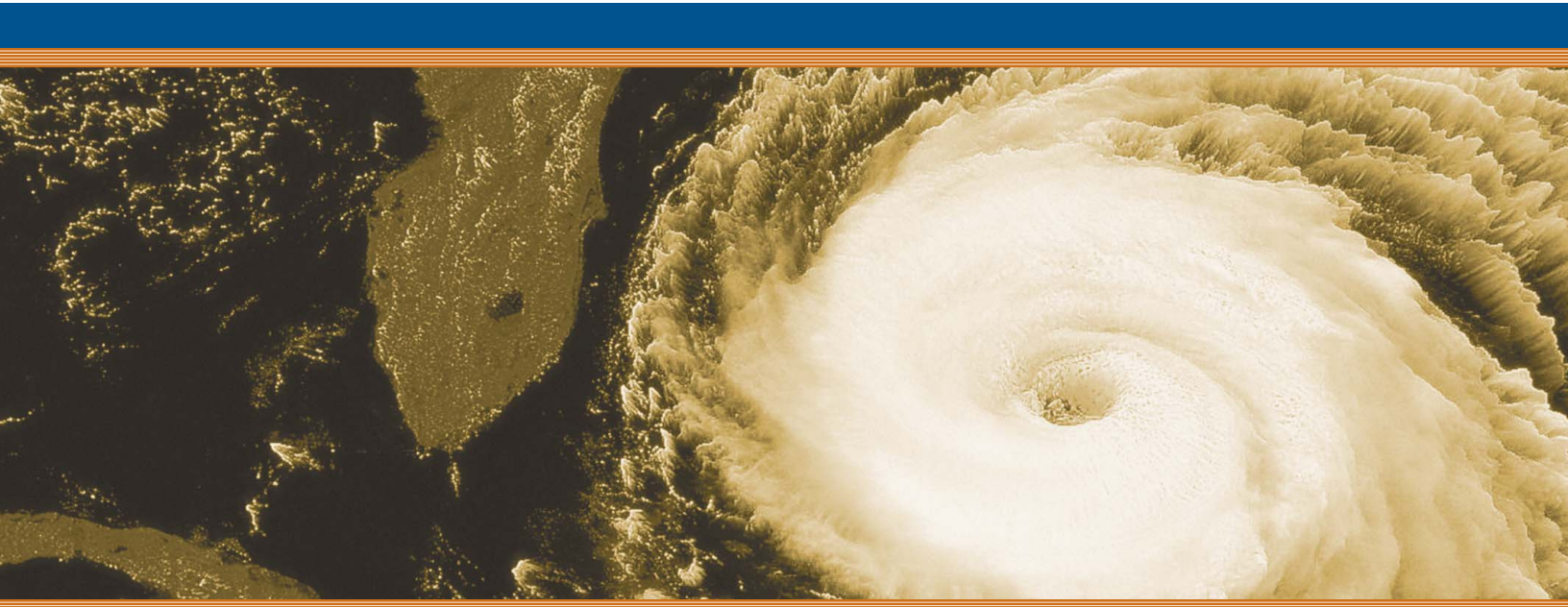


Executive Guide: Hurricane Preparedness 2006

Is Your Organization Ready?

Dorian J. Cougias



Contents

Overview	3
Before the Hurricane: Thinking About System Continuity	4
During a Hurricane Watch: Getting Ready	5
During a Hurricane Warning: Highest Alert.....	6
After the Hurricane: Facilitating the Disaster Recovery Process	7
Lessons Learned from Past Hurricane Seasons	9
About the Author	11

Executive Guide: Hurricane Preparedness

Is Your Organization Ready?

Overview

The 2005 Atlantic Hurricane Season 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. The heightened awareness of just how dangerous Hurricane season is for people and businesses cannot be understated. While experts are not predicting quite an active season this year, forecasters are predicting as many as 13-15 tropical storms and hurricanes in the Atlantic Ocean for the 2006 season which began on June 1st.

Businesses and organizations have a particular set of challenges during a hurricane. The safety and security of employees as well as damage to physical facilities and disaster recovery are major concerns. However, there is also the challenge of maintaining business continuity while minimizing short and long-term impact on your customers, suppliers, partners, and employees. Losing communication and critical IT systems for even a short time can have a significant impact on revenue, customer satisfaction and supply chain operations.

What can you do to ensure that your organization is prepared in the event that a storm incapacitates your office or offices? This executive guide, designed for senior administrative and IT managers, contains a detailed list of what you can do to prepare your organization before, during and after a hurricane. This guide also contains a list of valuable lessons learned from organizations that took action during past hurricane season to ensure a successful business continuity and disaster recovery process. As hundreds of companies have done during recent crises, these example organizations adopted Iron Mountain's Email Continuity Service (ECS) as well as its crisis communication system: AlertFind. In this guide, four companies share their stories and survival tactics on how they were able to "weather the storms" by minimizing the disruption to their operations.

The guide to hurricane preparedness contains several steps:

The following is a guideline of the steps you should take for your organization before the hurricane hits:

Foremost is communication and leadership! You will need to decide on a chain of command, keeping in mind that not all employees will act rationally during an emergency and that not all employees will be available or able to get in to the facility after the storm.

You will need to determine what should be stored off-site during a hurricane emergency and which computer systems and services will need to be kept running at a hot site.

Once complete, you will need to establish your plan and be sure that all staff are familiar with all parts of the plan, knowing what to do, when to do it, how to do it, and why they are doing it.

Finally, you will need to test your emergency communications plan. In an emergency, your staff will need to know that you are in charge and have a handle on the situation to help guide them.

Before the Hurricane: Thinking About System Continuity

The following is a guideline of the steps you should take for your organization before the hurricane hits:

- Conduct another walk-through of your organization's business continuity plan. Look for business and computing changes since the plan was originally implemented, last tested, or revised. Determine what changes in the plan may be required—and then make them.
- Check your hurricane and flood emergency action plan and update it as necessary. If there are changes, make new copies and distribute it to all staff members. Put a copy of the plan on a website hosted at your organization's hot site.
- Contact the National Flood Insurance Program (NFIP) (<http://www.fema.gov/nfip/>) disaster flood mitigation and insurance protection program. The National Flood Insurance Program makes federally backed flood insurance available to residents and business owners.
- Work with your state and local community, which should have a Hazard Mitigation grant. Authorized under Section 404 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, the Hazard Mitigation Grant Program (HMGP) administered by the Federal Emergency Management Agency (FEMA) provides grants to States and local governments to implement long-term hazard mitigation measures after a major disaster declaration. Hazard mitigation planning is an important aspect of a successful mitigation program. States and communities use the hazard mitigation planning process to set short and long-range mitigation goals and objectives. Hazard mitigation planning is a collaborative process whereby hazards affecting the community are identified, vulnerability to the hazards is assessed, and consensus reached on how to minimize or eliminate the effects of these hazards. In recognition of the importance of planning, States with an approved enhanced State Mitigation Plan in effect at the time of disaster declaration may receive additional HMGP funding. For more information, please visit the Planning website (<http://www.fema.gov/fima/planning.shtm>).
- Verify the operation of the standby generator, if present. Check that its fuel tank is full and that the fuel is uncontaminated (this should be done on a regular basis by the physical plant manager, but follow up with them —don't let it slip). Many companies who were adversely affected by the recent northeast power outage who thought they were "prepared" through the presence of a standby generator, found out after it was too late that they were short on fuel or that their supplies had become contaminated.
- Double check information with outside disaster recovery vendors or suppliers; notify them of any changes in your situation or needs. Cross check all of your services and costs with accounting so you will have the latest information.
- Make sure the building's grounds crew carefully trims all trees so they don't pose a threat to the facility. Ideally there will be no trees close enough to the building to cause direct damage. Dead wood should be removed to reduce wind-blown debris.
- Contact your insurance carrier and review your policy. They will also probably want to review your business continuity and disaster recovery plans. Make sure that replacement equipment or collections are covered. Ensure that copies of updated insurance papers are included in your disaster supplies—and are stored at your hot site for protection.
- Set in as many flashlights that you'll need around your office and data center. Count the number of flashlights you think you will need and then double the number that you actually put around. Mark your emergency flashlight positions on a floor plan that is kept off site (preferably as a part of your systems continuity and disaster recovery plan).

If you can't communicate, you can't lead and you definitely can't recover

- Test your emergency communications plan. Run through all of the “lifeboat drills” for communicating in an emergency with your key staff. Can you get a hold of key staff members through multiple channels (cell phones, pagers, home phones, remote office phones)? Can your emergency communications system escalate action items if key members can't be contacted within the prescribed amount of time?
- DO NOT merely run through the call system to desks or home phones. Test cell phones, BlackBerries and RIM pagers.
- Take people “out of the loop” and find out what happens to your chain of command if a link is broken. Can your emergency communications tool support-escalating problems? Can your team cope with a secondary leader taking charge?

Test your hot site's capabilities and setup

- Shut off access to your data center's communications and find out what should be located at your hot site that is geographically far enough away so that it isn't caught in any resulting natural disasters of its own.
- Review previously established safe havens inland where you plan to send priority collections and other important data. Verify that they are still operating and accessible.
- Review previously established “remote work sites” inland where you plan to convene key staff and equipment. Verify that all data connections are intact and working properly.
- Test the ability of your secondary team members to work remotely. Then begin testing the ability of other team members (from the most important to the least) to work remotely through VPNs and other means.

During a Hurricane Watch: Getting Ready

A Hurricane Watch is issued when there is a threat of hurricane conditions within 24-36 hours.

- Initiate your emergency communications “hurricane watch” plan. Ensure that you have communicated with everyone on the list and that they can all both send and receive communications through email and voice systems.
- Free as many staff as possible from routine duties, even if this means announcing that your institution is closing to the public to begin preparations.
- Listen to a battery-operated radio or television for hurricane progress reports.
- Secure buildings by closing and boarding up windows. Remove outside antennas. Take in all loose objects on the grounds—benches, birdbaths, art works, anything that is bolted to concrete.
- Secure trashcans, gates, and garden hoses. Take down awnings and other items that may blow away.
- Turn your data center HVAC system to its coldest settings in case you have to “dump its load” to keep your UPS systems powering critical computers.
- Notify outside contractors and your hot site that you may be calling on their services in 24 to 48 hours. This will alert them to begin monitoring your situation. Ensure that they are a part of your emergency communications plan.

- Store valuable organizational papers in waterproof containers on the highest level of your office. If you are going to use off-site storage of high priority collections and data, begin packing now. You should have arranged to rent a sufficient size van or truck (you should have already worked out payment details, driver, size of vehicle needed, and company). The vehicle should be automatic shift, have air conditioning, and an AM/FM radio. Be sure to have a first aid kit and fire extinguisher put in the cab. At this point, your safe destination should be your hotsite or remote inland worksite.
- If you are going to continue working, review the evacuation plan and emergency communications plan.
- Begin preparations in the building. Have staff members clear their desks. All papers, files, collections, and other materials must be put under cover. At this point basic patron services must be terminated.
- Identify shelters established by the city and make sure this information is distributed to all staff members—just in case they need the assistance. Make sure that elderly, pregnant, or disabled staff members have assistance and release them from further duties.
- Fill water storage containers and make sure they are stored in two different areas of the building in locations where, if they rupture, collections will not be damaged.
- Make sure all of your institution’s vehicles are filled with gas. It is also a good idea to install locking gas caps, since others will steal gas during an emergency.
- Refresh the staff regarding their responsibilities after the storm is over. Make a determination of when different staff members should report to work (you probably won’t want everyone coming in all at once, before the assessment of damage is completed). Make sure everyone knows what they are supposed to do after the storm—there will be little hope of communicating with all your staff during the first 48 hours after a storm, so plan ahead.

During A Hurricane Warning: Highest Alert

A Hurricane Warning is issued when hurricane conditions (winds of 74 miles per hour or greater, or dangerously high water and rough seas) are expected in 24 hours or less.

- Initiate your emergency communications “hurricane warning” plan.
- If power to the area is lost, manually unplug (do not just turn off) all computer systems that are not needed. The reason you want to unplug them instead of turning them off is to avoid any potential problem of a power “surge” when electricity is restored.

If officials indicate evacuation is necessary:

- Initiate your emergency communications “hurricane is hitting” plan.
- Leave as soon as possible. Avoid flooded roads and watch for washed-out bridges.
- If you can, have building maintenance turn off main electricity and the main water valve.

- If time permits, and you live in an identified surge zone, elevate all key paperwork and computers to protect them from flooding. Better yet, move them to a higher floor if you have one. If possible, move collections away from windows (this becomes even more important if you don't have hurricane shutters). Move collections from bottom floors if there is any potential for flooding. Take second priority collections to the safest locations in the building (preferably interior rooms or rooms with no windows which are not on top floors) and cover with plastic sheeting. Securely tape this sheeting so it won't blow off.
- Brace double doors and garage or loading dock doors. Limit building access to one or two points as the others can be shut down. Caulk under doors—any place that water could enter. Silicone caulk will easily peel up afterwards.
- Obtain several hundred dollars in petty cash for post-hurricane emergency supplies.
- Take half of your institution's vehicles to a public parking garage. While flying debris may damage them, these facilities are typically well built and are likely to withstand even major hurricanes. You may not be able to retrieve the vehicles for several days, but this will at least maximize their potential for survival. Vehicles left at your facility should be put under cover if possible. If there is no cover, park the vehicle as close to the building as possible—that way at least one side may be protected from wind and flying debris. Try to anticipate the direction of the wind and park the vehicles on the downwind side.
- Cover all desks, computers, copiers, and other equipment with plastic sheeting. Securely tape this down by running tape around the items.
- If your institution has any rooftop items (antennas or satellite dishes), remove them if possible.
- If there is a staff lounge with a refrigerator, turn it to the coldest setting. If your facility has a walk-in cooler, turn it to the lowest setting.
- Based on last-minute weather bulletins and the advice of local authorities, determine if there is a need for staff to stay in the building. If not, all staff should leave the institution, securing the last hurricane shutters as they leave. Be sure to leave power to essential equipment (security, fire, emergency lighting, and environmental controls) on. The rest can be cut off. Likewise, if your HVAC system does not use gas, but there are gas lines entering the building, shut them off at the main.
- Lock up the building and leave.
- Advise police and fire chiefs of your status.

After The Hurricane: Facilitating the Disaster Recovery Process

Once you know the hurricane is over, you'll need to switch gears. Again, go back to that communications plan and enact your recovery scenarios. Get someone on site as quickly as possible to assess the damage and prevent vandalism or theft if the damage is great enough to allow it.

Enact your "disaster recovery" communications plan

- Your disaster recovery plan should have a set of steps for recovery, beginning with a recovery communications plan, hot site de-integration plan, and restoration procedures for normalizing staff activities.
- Communicate as you proceed. Not everyone will know that you are "on track," so keep communications flowing. Let all staff know how the progress is coming and give them the next milestone in the recovery plan to look forward to.

- Enter your building with caution. Beware of snakes, insects, and animals driven to higher ground by floodwater.
- Take pictures of the damage, both to the building and its contents for insurance claims.
- Look for electrical system damage. If you see sparks or broken or frayed wires, or if you smell hot insulation, turn off the electricity at the main circuit breaker (if you didn't do that before leaving the building). If you have to step in water to get to the circuit breaker, call the building electrician first for advice.
- Check for sewage and water lines damage. If you suspect sewage lines are damaged avoid using the toilets and call the facility plumber. If water pipes are damaged, contact the water company and avoid the water from the tap.
- If you have a raised floor in the data center, and the data center is on the ground floor (or below), lift the floor panels and check below them for leakage or flooding. If you have power cables running under the floor as well as data cables, think twice before you power up the systems. When in doubt, don't be a hero.

The second biggest problem will be the water

- Locate hidden water damage through taking moisture readings around window casings, exterior doors and roof vents, etc.
- Speed is the most important! When the water source has been eliminated, professional extraction must begin immediately to prevent health hazards and further damage. Restorative drying will need to be completed including a mildew-cide treatment.

The third problem will be prevention of further damage or vandalism

- Most insurance companies state that, "...the insured is responsible for taking any reasonable and prudent steps necessary to preserve, protect and secure the structure and contents from further damage." Of course you can't stop a hurricane. But you will need to take steps toward limiting further damage due to continued hazards, theft, or vandals. Your second efforts (after or during water removal) will be to "contain" any potential damage; protect and secure your property and computer systems from weather and other factors as much as possible. This will need to be accomplished even before an adjuster has the opportunity to survey the damage.

Lessons Learned from past Hurricane Seasons

In today's global business world, even a hurricane is not an excuse for a company's business lifeline to be compromised. As record numbers of hurricanes ripped through Florida and the Gulf states over the last two hurricane seasons, Iron Mountain's Email Continuity Service (ECS) and AlertFind provided email continuity and emergency notification services to many tens of thousands of employees and constituents across the state. Email has become an absolute mission critical business application. During the numerous hurricanes, Iron Mountain customers sent and received more than a million email messages through the ECS. At the same time, AlertFind enabled organizations to transmit hundreds of urgent messages to their employees and other critical personnel.

As businesses and organizations of all kinds learned last year, it pays to be prepared. Below are the tactics used by various organizations that took steps to be prepared and how they managed during the storms:

Adams and Reese LLP: Kept communication up and running during Hurricane Katrina.

When Hurricane Katrina struck in the summer of 2005, most companies in the Gulf faced with were minimally prepared. Adams and Reese, one of the largest law firms on the Gulf Coast, is headquartered in central downtown New Orleans and has offices in Alabama, Mississippi, Texas, and Washington, DC. The firm's 300 attorneys provide legal support to clients globally.

Adams and Reese had put in place Iron Mountain's Email Continuity Service (ECS) to ensure email and BlackBerry communication regardless of the state of their Microsoft Exchange server. ECS is a stand-by email continuity solution that automatically synchronizes with the Exchange environment and can be activated within 60 seconds for continuous corporate email communications regardless of any outage. As a managed service hosted at Tier 4 secure data centers throughout the world, ECS can be implemented in under an hour and activated on-site or remotely—by phone or through an Internet connection.

When Katrina hit, 250 Adams and Reese employees were located in the New Orleans headquarters building. During the evacuation process, the power, then the battery backup went out, and before the Exchange servers lost power, Adams and Reese CIO, David Erwin, failed over corporate email to ECS. The firm had no lapse in email communications between employees and with clients throughout the disaster.

After the Exchange system was back up and running, all email communications that occurred during the ECS activation were restored to the primary Exchange server—along with all forensic information, such as sent and received times. ECS also synchronizes all calendars, contacts, and historical messages for a specific retention period to provide complete continuity for end users.

Holland & Knight, LLP: Advanced preparation ensures a crisis in Florida does not affect critical global communications.

With global headquarters in Tampa, Florida, the law firm's more than 3,500 partners, attorneys and staff depend on email to communicate with clients and one another across their 10 Florida offices, 17 U.S. offices, as well as eight international offices that span the globe. Holland & Knight had implemented Iron Mountain's Email Continuity service (ECS) as "insurance" against any power or email system outages. This was a critical step of preparation since an email or power outage in Florida could precipitate a communications breakdown across all of the firm's offices. ECS is hosted in secure offsite data centers and, when activated, provides employees continuous access to their corporate email through and Internet connection. They can continue to send and receive messages and access historical email, calendars, and all contact information.

In the wake of hurricane Charley in August of 2004, Holland & Knight experienced a power shutdown in its Tampa and St. Petersburg offices. They quickly activated ECS backup email system to enable the more than 200 lawyers and staffers to continue to send and receive corporate email from remote locations despite the firm's email servers being down.

"Holland & Knight is focused on providing world-class client and support 24x7. As one of the largest law firms in the world, we need the ability to communicate via email, no matter what," said Ralph Barber, CIO of Holland & Knight, LLP. "We've come to rely on the emergency mail system and they've not let us down. Hurricane Charley was no exception, we're confident that with ECS, we will always have email."

Global Berry Farms: A location unaffected by the storm enables email continuity for Florida employees.

In preparation for Hurricane Charley, the leading grower/shipper of berries: Global Berry Farms purchased and rapidly deployed ECS during the week preceding the hurricane. They realized that with the storm on the way, they need a solution that could rapidly deploy without disruption their IT operations. ECS can be installed in 60 minutes for an entire multi-divisional organization. A mid-sized multinational company, Global Berry Farms is headquartered in Naples, FL with satellite offices in Michigan, California and Santiago, Chile.

Once Charley hit, email systems went down in Naples. Global Berry's staff in Michigan was able to work directly with Iron Mountain to activate the ECS for its critical Florida users. Global Berry's IT environment includes two Microsoft Exchange servers—one in Naples, one in Grand Junction, Michigan. Global Berry staffers leveraged ECS for 14 hours, to send and receive email, during the power outage.

"When hurricane Charley hit Southwest Florida, our phone system, T1 data line, and power went down, but the ECS email system was available to all of our employees across the country, despite the hurricane," said Brian Clancy, MIS Manager, Global Berry Farms. "We thank them for a job well done."

Blue Cross Blue Shield of Florida: Frequent emergency communication keeps employees informed.

Affected by three of the major hurricanes to hit Florida in 2004, the insurance company relied on Iron Mountain's AlertFind emergency notification and escalation service to notify tens of thousands of employees, partners and clients on critical updates regarding office closures, evacuation orders and updates to business continuity and resumption plans.

As an automated notification system, AlertFind enables disaster recovery, human resources, and other management personnel to instantly broadcast critical messages to employees cell phones, PDA's, pagers, and other devices. In addition, it enables two-way communication enabling alert recipients to reply to a poll or to a call to action during a crisis if they are emergency personnel.

Blue Cross Blue Shield of Florida sent over 200 separate emergency notifications throughout the weeks that the hurricanes hit, keeping employees and others fully informed about every aspect of their situation.

Summary

With a worse than average hurricane season predicted for 2006, Iron Mountain stands by at highest alert levels to assist organizations in preparing for continuity of operations and then delivering the most rapid, widely proven, and cost-effective solution to meet their needs. Whether you are a public agency, a law firm, or a corporation, you will have a need to communicate and maintain your operations in ways and situations that are as unique as the examples above. These organizations that shared their stories exemplify a range of different situations and different risks despite all being hit by the same storms. Iron Mountain encourages you to contact us and we'll work together with you to determine your unique storm survival strategy.

About Dorian Cougias

Dorian Cougias is the founder and CEO of Network Frontiers, a company that focuses on disaster recovery, security, and IT infrastructure consulting, training, and publishing. Over the last 11 years, Dorian has written and spoken extensively on technical topics, has served as CIO of two of the world's leading ad agencies, and has been the continual vision behind Network Frontiers. He is a best-selling author of more than ten books including the recent third edition of *The BackUp Book: Disaster Recovery from Desktop to Data Center*. Dorian also serves as a Professor of Computer Science at The University of Delaware as well as continuing to consult for clients with significant data management requirements. He works closely with application developers and with hardware vendors to ensure that the IT community understands their products' benefits and, in turn, that the vendors address administrators' needs.

©2006 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated. All other trademarks and registered trademarks are property of their respective owners.



745 Atlantic Avenue
Boston, Massachusetts 02111
800-888-2774

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the U.S., Europe, Canada, and Latin America. For more information, visit our Web site at www.ironmountain.com