

Managing Computer Room Disasters with OFirst Alert Procedures and O4Ci



By [Leo Wrobel](#), [Sharon Wrobel](#)

Date: Dec 1, 2008

[Return to the article](#)

Would you know what to do if you strolled past the computer room after hours and saw water coming under the door? Leo A. Wrobel believes that every organization needs a disaster plan that includes designated instructions for a first responder and the emergency team that gets the first phone call.

Every organization should have some type of business resumption plan in place, designed to respond to disaster. The term disaster, as defined in this article, breaks down into four categories:

- Natural damage
- Intentional harm
- Human error
- Acts of God

Any of these events that eliminate or severely impair a mission-critical function of an organization are assumed to be a disaster. Therefore, the definition of a disaster varies by organization. Various entities have different "pain thresholds" that define when an incident becomes a disaster. A bank, for example, will have different criteria than a poison-control hotline. With this fact in mind, any organization should begin the process of implementing "first alert" and response teams after it has completed a [business impact analysis](#) (BIA), preferably with the help of a reputable consultant. Your BIA should establish your organization's essential criteria for recovery timeframes: how quickly the organization should respond, and therefore how the first alert procedures should be structured.

First alert procedures for any recovery plan should provide for specific recovery tasks, including checklists, forms, and procedures required to allow assigned personnel to effect a timely recovery. All first alert procedures depend on communications. This article addresses the practical principles for how to develop such communications between responders, including but not limited to the following:

- Designation of specific, responsible personnel as "first responders" to disasters.
- Identification of teams responsible for initiating emergency recovery activities
- Standards and procedures to maintain command and control in a recovery effort
- How to communicate effectively with responders, and appropriate technologies to use for that purpose.

First Alert Procedures

Business resumption and disaster recovery are placed into action through a documented first alert process. The purpose of this process is to ensure that management is informed of a disaster at the facility immediately after discovery of the situation. Documented procedures and checkpoints are written into the disaster recovery plan, including an initial assessment of the damages. This all-important initial report provides responsible management with the information they need to answer an all-important question: "Do we declare a disaster or not?"

Since disasters come in all shapes and sizes, the people who first discover and report them also come in all shapes and sizes. Often the message doesn't get through to the right people. For example, people in an information technology department might have the impression that they'll get word of a problem first. In reality, this is more of an exception than the norm. For example, a night security guard or building facilities staffer might be the first to discover water coming under the door of a critical computer room. This is another reason why it's important to have first alert procedures. Such procedures must transcend the various departments in a large organization to ensure that the right people get the word immediately, no matter who discovers the problem.

It's impossible to cover all aspects of a good first alert process in a single article, but let's consider a few technologies that can enhance and streamline the first alert process:

What Happens If You Are the First Alert Person?

In theory, any employee should be prepared to be a First Alert person and to assume first alert responsibilities. Here's how the process should go:

1. The First Alert person notifies one of the Initial Disaster Response Personnel listed in the recovery plan. Obviously, your recovery plan should be in an accessible location in order to achieve this goal. It's also prudent to keep critical information in a personal digital assistant device (PDA), BlackBerry, or cell phone where it will be accessible when needed and where it will be more likely to stay up to date.
2. The first person that the First Alert person should contact is sometimes called the Disaster Verifier. The Disaster Verifier refers to a predetermined section of his or her disaster recovery plan, which should include a form for determining the following details about the event. (It's important that the Disaster Verifier obtain this information while still on the telephone with the First Alert person)
 - Date
 - Time
 - Name of the First Alert person
 - Wireless phone number of the First Alert person
 - Location of the event
 - What happened?
 - Initial estimate of damages and injuries
 - Is the building accessible (yes/no/partially)?
3. Before hanging up from the initial call, the Disaster Verifier should arrange to meet the First Alert person at a designated location.
4. Before hanging up from the initial call, the Disaster Verifier should remind the First Alert person not to make any public statements regarding the situation.
5. Now the Disaster Verifier takes over responsibility, notifying a predefined Recovery Management Team (RMT) that a disaster has occurred. Theoretically, the Disaster Verifier should start by notifying the Recovery Management Team Leader; however, if that individual is unavailable, the Disaster Verifier should go down a prearranged list in order as shown in the following table. Any designated team leader should be prepared to perform in the absence of any other. Remember, an event may occur on a holiday, or when key personnel or vacation; worse yet, some of the Recovery Management Team may themselves have been affected by the disaster. The table offers suggestions on other recovery teams you may want to consider.

Title/Team	Person Contacted	Home Phone	Time Contacted	Result of Contact
Recovery Management Team (RMT) Leader				
Affected Site Team Leader				
Offsite Data Storage and Retrieval Team Leader				
Building and Facilities Team Leader				

Equipment Installation Team Leader				
Equipment Recovery Team Leader				
Systems Software Team Leader				

- 6. The Disaster Verifier and Recovery Management Team contact evaluate all information obtained thus far and decide whether a true disaster situation exists. If all facilities, equipment, and data are unaffected and the problem can be resolved easily by operations personnel as well as vendor systems engineers, the two then cancel the alert. If this is not the case, however, it will be necessary to implement the disaster recovery plan
- 7. If the disaster recovery plan is to be implemented, it's time to alert the boss

The first thing that will be needed is a media statement to prevent panic and to stay in control of the situation. An example might read as follows:

INITIAL MEDIA STATEMENT

The emergency is being handled in accordance with established emergency procedures. Our management team is meeting with the local authorities right now to obtain official information related to the incident.

- 1. We want you to publicize the facts regarding the situation
- 2. Management will be presenting a statement very shortly. You will be invited and escorted to the location.
- 3. The situation is under control
- 4. We will hold a press conference at [insert time and date] with updated information as to the status of the disaster.

In addition to statements designed for people outside your organization, think about how you'll communicate with people inside your organization. It's important as a contingency planner to communicate to others involved in the recovery process using terms that they understand. Engineers, for example, like schematic diagrams of a process. Building managers often prefer equipment layout diagrams and floor grid diagrams. Programmers and managers might prefer flowcharts like the one in [Figure 1](#).



[Figure 1](#) Adapted with permission from Leo Wrobel's upcoming book Business Resumption Planning, Second Edition (CRC Press, fall 2008).

The Importance of Command and Control (4Ci) to the First Alert Process

Command and control are of the utmost importance throughout the first alert process since rapid decisions must be made in a pressure situation based on what must be accurate information. The military uses the expression 4Ci for the elements of this process:

- Command
- Control

- Communications
- Computers
- Intelligence

After all, most of the mission of the military involves responding to catastrophic unexpected, and potentially deadly situations. In order to respond appropriately, however, the person or people in charge must have accurate knowledge of the situation. [1] Solid communications are crucial to conveying that information to decision makers in order to have any semblance of command and control. [2]

Any means of maintaining 4Ci in a disaster is a survival advantage. Options as mundane as laptops, BlackBerry devices, wireless phones, instant messaging, voicemail, broadcast fax, email blasts low-power radio stations two-way radios, and push-to-talk phones add immeasurably to the capability of 4C

NOTE

Commercial, nongovernmental, and nonmilitary organizations today demand a military level of 4Ci. Recognizing this shift in attitude, I've coined a phrase for that idea: b4Ci. The b in this case stands for business.

Many technologists in the U.S. and China are military veterans, with experience that's now useful in the private and nonmilitary sectors. Others have served as firefighters, emergency medical technicians (EMTs), police officers, or in other capacities in professions that deal with rapid responses of one type or another in disaster situations. It's possible to draw on this kind of experience when addressing an organization's business resumption plans, disaster recovery plans, and first alert procedures

The first step in that process is to think through what would have to happen in response to a given situation. Who would need to come to work immediately? Who would be required to stay home, to avoid being in the way? What if key people couldn't or didn't show up who would replace them? Worse yet, what if key people were injured or killed? Who is responsible for calling employees to work? How would this responsible person contact those employees? What backup means are available for contacting staff if telephone, cell phone, etc. are not available?

So where do you begin? What are the enabling technologies that allow for powerful, well-defined, yet flexible first alert procedures?

First, get your thoughts and facts rolling by thinking about questions like the following (presented in no particular order):

- Where is your meeting place if the affected building is inaccessible?
- Who will comprise your initial response teams?
- How will you contact your initial response teams?
- What happens if these people are not available?
- How do you document call-out numbers?
- How do you keep call-out numbers up to date?
- Where are all your emergency numbers?
- Who do you call in case of injury or death?
- Who will speak to the media?
- How will your customers/clients/patients, etc. react?

Once you have the fundamentals down, consider which technologies you can use to augment your first alert procedures. Selecting the right technologies makes your first alert procedures more powerful and yet more flexible in their ability to respond to changes in situations. Consider the following possibilities:

- Wireless phones
- Voice conference bridges
- Two-way radios
- BlackBerry devices
- Laptop computers
- Push-to-talk phones
- Broadcast fax machines
- Fax servers
- Offsite hosted email accounts
- Offsite hosted voicemail accounts

- Satellite phones
- "Black box" wireless-to-landline adapters
- VoIP phones

Once you've organized the fundamentals, many enabling technologies are available to help you develop a level of precision and sophistication in your first alert procedures that rivals a NASA space shot.

These are the most important things to remember

1. Know your business by conducting an effective business impact analysis with the help of a reputable outside source.
2. Set your first alert objectives based on the particular makeup of your organization
3. Enable and empower your first alert procedures with available supporting technology

I hope that these tips helped you. I wish you the best of luck in your contingency planning pursuits

Leo A. Wrobel is honored to be a speaker at the first International Workshop on Emergency Management Technology, Application and Practice (EMTAP 2008) in Beijing, China November 14-15, 2008. The conference is sponsored by the Chinese Academy of Sciences (CAS) Institute of Policy and Management (IPM) and the Pacific Disaster Center.

Footnotes

[1] In the days of the Cold War, U.S. war planners had to be able to distinguish whether a heat bloom was a gas well or a missile launch. In such situations, a "false positive" and a "false negative" could be equally catastrophic. This is why not only communications was important, but the quality and accuracy of the information received by decision makers. The same holds true with today's disaster recovery planners

[2] The U.S. military has often invoked an old saying, "No battle plan stands firm against contact with the enemy." This is a universal truism that is applicable to any military force, and translates (at least conceptually) to any language. It probably dates back in spirit 50,000 years, to the days of cave men running terrified from a well-planned battle screaming, "They have clubs!" Unexpected things happen in battle, and situations change from what was planned. The same principle applies when planning for handling business disasters
