White Paper

Using Incident Notification in a Disaster
Using Incident Notification in a Disaster

Introduction

In recent years, Americans have been dealt repeated shocks to their sense of security. Natural disasters such as floods, earthquakes, and wildfires, as well as manmade disasters such as shootings, blackouts, and terrorist attacks, have made us all aware of the potential for sudden, large-scale damage and disruption of our regular lives.

Businesses and government agencies have begun to analyze past disasters with increasing urgency, and are now systematically preparing responses to future disasters. Today, many large organizations have business continuity managers working on these issues full time, and a growing body of literature addresses the best ways to prepare for and respond to disasters.

A great deal is at stake. For government agencies, the primary concern is public safety: containing the threat, moving people out of danger, sheltering those who have been displaced, and rescuing the injured. The quality of disaster preparedness and response can be measured in terms of lives lost or saved.

Businesses in a disaster area may be asked to coordinate with public safety agencies by evacuating employees or accounting for their whereabouts. But employee safety is not businesses’ only concern. They must also restart their operations as quickly as possible, whether this means relocating to a temporary site, bringing in backup power or other services, repairing damaged buildings or equipment, or recovering data from computer systems.

Often, business viability is at issue. It’s estimated that two out of five enterprises that experience a disaster go out of business within five years\(^1\). Sometimes the loss of key personnel cripples the business. In other cases, recovery costs may be overwhelming, or customers may switch to other providers or simply lose confidence in a business’s ability to recover.

Communication is Critical

Mobilizing resources is not the greatest challenge in responding to large-scale disasters. Research shows that no matter how shell-shocked people are, they nearly always rise to the occasion. Both trained and untrained people assist as best they can with rescue and recovery efforts, and they are willing to follow the directions of those who are coordinating the disaster response.

Rather, every analysis of past disasters points to communications as a limiting factor in disaster response. In many instances, communications failures have been blamed directly for adding to the toll of death and destruction.

\(^1\) Gartner Dataquest, AV-14-5238, 2001.
This should not be surprising. Responding to a disaster involves assessing the damage and the continuing danger, issuing instructions to those at risk, and coordinating the assistance activities of large numbers of people. Communications are central to all these tasks.

To improve disaster preparedness, business and government officials need to make communications systems more reliable. One important piece of the puzzle is incident notification – automated systems that send voice and/or text messages to large numbers of people at once. A well-designed incident notification system can prevent many of the communications failures that hamper disaster recovery.

**“Battle in Seattle”**

**The 1999 World Trade Organization Ministerial Conference**

Trade ministers from more than 130 governments gathered in Seattle, Washington in November 1999 to develop a global trading framework for the 21st century. Conference planners didn’t anticipate that 50,000 demonstrators would also converge there. A high-profile event turned into a powder keg. Outnumbered police struggled unsuccessfully to contain rioting protesters. A state of emergency was declared; 56 police officers and almost 100 demonstrators were sent to the hospital. The demonstrations cost the City of Seattle and supporting agencies an estimated $20 million dollars.

An incident notification solution would have helped authorities confront with order and efficiency the challenges posed by the demonstrations.

- The FBI, Secret Service, and FEMA were originally enlisted to protect the event from terrorist threat – and the unexpected violence only made their jobs more difficult. With an incident notification system, they could have received real-time situation updates and used conference calling to coordinate action.

- Active-duty military specialists were deployed because of their expertise in biological and chemical attacks, explosives disposal, and counterterrorism. Incident notification could have alerted these teams to developing threats and provided the exact details necessary for them to save lives.

- The California Army National Guard was called out to help maintain order. Members could have instantly been recalled to their duty stations and told to prepare for deployment throughout the city.

- Seattle police were stretched thin and operated in a fog of confusion. Automated notification could have provided them necessary situation updates and helped coordinate police efforts to diffuse violent flash points.

- With incident notification, Seattle city managers could have alerted city workers to the danger posed by rioting crowds and directed them to alternate work sites, helping maintain continuity of government (COG).

- The news media could have used a notification system to rapidly direct news and camera crews to developing events.

- The conference organizers were at the center of the storm, dealing internally with the ongoing crisis and externally with law enforcement and media. Incident notification could have ensured maximum flow of information among organizers and allowed them to deliver consistent messages to multiple information seekers.
Why Communications Fail During Emergencies

Responding to a major disaster is such a complex process that communications can fail at many points along the line. Following are some of the types of communications failures that have been identified in recent emergencies. Many of the cases experienced cascading failures, where one type of failure actually led to another.

Communication systems are damaged

Network theory tells us that networks can usually survive random faults and outages, but that they will collapse when even a small percentage of the largest hubs are damaged or removed. Communications depend on two types of networks – the lines and switches that carry communications signals, and the electric power grid. If major hubs for either of these networks are disabled, a systemic communications failure may result.

In one tragic example, the 1995 earthquake in Kobe, Japan destroyed most communications links. Local officials could not reach fire or rescue units for days, and they could not request assistance from other cities. Officials of nearby cities and the military were reluctant to send assistance without an official request, even after it became apparent that Kobe had suffered massive destruction.

Some other recent examples:

- Wire line telephone service, broadcast radio, and television were disrupted in the 2001 World Trade Center (WTC) attack. Telephone service was restored gradually, and in some cases, lower-priority customers actually lost service during the days following the attack so that service for higher-priority customers could be restored.

- In May of 1998, 90% of the 40-45 million paging customers in the United States lost service when a communications satellite malfunctioned and left its normal earth orbit. Virtually every pager company in the country was affected.

Some organizations are now trying to insure themselves against systemic failures by building their own redundant systems – for example, by contracting with multiple wire line and wireless telephone carriers and Internet service providers, constructing in-house cellular antennas, and arranging for calls to be rerouted to an alternate site if necessary.

There are two problems with this approach: First, it’s expensive. And second, it addresses only one end of the communications link. Being able to make telephone calls is of little use if the people you are trying to reach can't receive them.
Communication equipment isn't functioning

Even when there is no systemic damage, localized problems may interfere with communications. The point of failure can often be individual pagers, cell phones, or radios.

Power requirements for these devices are much greater when they're under heavy use. And since they are useful only when they are left on, conserving battery power in a crisis is not an option. A cell phone battery may last for two days or more when it is used intermittently, but in the continuous use brought on by emergency, it will last only a few hours.

When the crisis is a blackout or power failure and batteries can't be recharged, cell phones can quickly become useless. During the 2003 Northeast blackout, companies tried to contact their employees via cell phone and found, to their frustration, that even when the cell network was functioning they couldn’t speak with employees and had to leave voicemail messages that the employees could not retrieve.

Communication lines are overloaded

Overloading can occur for two reasons: unusually high traffic or damage to parts of the system.

When disaster strikes, people immediately pick up the telephone – to find out whether their friends and relatives are safe, to rearrange their plans, or just to find someone who knows more than they do about the situation. These calls may so overload the system that most calls just get busy signals. So even when there is no damage to the telephone system or equipment, it may be impossible to make the calls needed to arrange disaster response. This occurred in the aftermath of the 2001 earthquake in Seattle, Washington, when telephone service was overloaded for two days and more than seven million telephone calls were rejected.

If portions of the system are damaged in the disaster, the situation is even worse. When traffic is shifted to the undamaged portions, these may quickly become overloaded and even shut down. The more nodes become unavailable, the more overloaded and vulnerable the remaining nodes become. Network theorists call this a cascading failure. A cascading failure took place during the 2003 Northeast blackout (which was itself caused by a cascading failure of the electric power grid), when the functioning parts of cellular and landline phone systems became overloaded.

Overloading at a local level

Overloading can also occur at the level of the organization, either because local telephone equipment such as a PBX is overloaded or because not enough staff are available to answer telephone calls. The volume of calls coming in to a company or government agency may block urgent calls that are needed to arrange disaster response.

- After Hurricane Isabel struck the East Coast in 2003 and knocked out power lines, a Delaware electric utility received three months’ worth of telephone calls in four days. The
company’s automated answering system disconnected many of the callers, including some who should have been candidates for high-priority restoration.

• Radios, especially older models or radios on older networks, are vulnerable to interference and channel conflicts. Emergency responders sometimes find themselves trying to talk at the same time or even dealing with “bleed over” from nearby channels. Communication intended for specific individuals or groups must be broadcast to everyone on the radio network, and their simultaneous responses further clutter the channel.

• Emergency Medical Systems chiefs responding to the 2001 attack on the WTC were hampered by the large volume of radio traffic. This made it hard for them to understand the overall situation at the disaster site, and several attempts to conduct a roll call of chiefs failed. Even when a second radio channel was opened for dispatching ambulances, the chiefs continued to have trouble communicating with one another.

Multiple agencies can't communicate with each other

First responders to a disaster frequently rely on handheld radios for on-the-scene communications. However, when multiple agencies arrive on the scene, they are often literally on different frequency bands and cannot coordinate their efforts. Technical solutions to this problem exist, but they are often expensive and cumbersome to install.

• Incompatible radio frequencies prevented police and fire teams from communicating when the World Trade Center towers were collapsing in 2001, and may have contributed to the deaths of some firefighters.

• In the 2003 California wildfires, responders said that incompatibility between local and state agency radios affected safety and operations more than any other issue. Some “burnouts,” or deliberately set fires, had to be started without consulting with neighboring localities.

In addition to technical communications problems, the involvement of multiple agencies can cause other sorts of communications problems. The 2003 California wildfires spread so quickly through so many jurisdictions — more than 50 in San Diego County alone — that agencies effectively stopped communicating and focused on their own geographic areas.

The disaster coordinator’s location is inaccessible

In a disaster, important buildings may be destroyed, damaged, or otherwise inaccessible (for example, if buildings all around them are burning). Municipal command centers were destroyed during both the 2001 World Trade Center attack and the 1995 earthquake in Kobe, Japan. Some financial institutions could use neither their primary nor their backup headquarters in the aftermath of the 2001 World Trade Center attack, because they hadn’t planned for a region-wide disaster and had located the two sites too close together.
If the disaster recovery plan is dependent on access to a particular site – for example, if the only communications link or the only copy of the contact lists is in that site – then coordinating the disaster response can be extremely difficult.

**People aren't where they were expected to be**

During a disaster, people move around. Trained personnel may head for the disaster site, thinking that they can help; people who are already at the site, but are not in a position to help, try to go home. If transportation problems keep people from arriving where they intended to go, disaster coordinators may not know where to find them.

During the 2003 Northeast blackout, many workers in New York City who depended on public transportation spent the night camped at friends’ apartments or other ad hoc shelters. Their employers had difficulty contacting them to tell them whether (and where) to report for work the next day.

**Contact information is out of date**

A critical aspect of business or government continuity planning is maintaining up-to-date contact information for everyone who must be notified or summoned in an emergency. Searching for phone numbers during an emergency wastes precious time, sometimes with life-and-death consequences.

In the 1989 California earthquake, San Francisco’s 911 system was disabled and police had to switch emergency calls manually. They quickly discovered that their telephone numbers for outside agencies and departmental units were wrong or outdated, leading to delays in responses to emergency calls.

**One-on-one communication takes too long**

Even when disaster coordinators can locate the people they are looking for, reaching all of them may be a slow process. The time it takes to call them or find them in person can hamper disaster response and recovery. Personnel are also distracted from other tasks by having to spend time trying to contact people; for example, firefighters who are checking to see whether residents have evacuated a neighborhood are not available to fight the fire.

Some examples include:

- Many business continuity (BC) managers had to work round the clock after the 2001 WTC attack to reach critical vendors and support personnel so they could bring systems back up and restore primary or alternate sites.

- Seventeen people died during the 2003 wildfires in Southern California, some because firefighters going door to door could not evacuate them from their homes quickly enough.
• During the 1999 Columbine High School incident, the police could not communicate while the shooters continued to attack students and teachers inside the school. Later, when wounded victims were being evacuated, the lack of timely information hindered the hospitals in their preparation of emergency resources. Hospitals had to look to the media for information, and as a result they had difficulty keeping media reporters from intruding on victims’ privacy.

Sometimes the time-consuming nature of one-on-one communications leads emergency coordinators to make decisions they might otherwise not have made. For example, in the Columbine High School incident, school officials had to keep students who had been evacuated from the school in the gymnasium of a local elementary school so that they could continue updating them on the situation. Even students who had been reunited with their parents were not permitted to leave until evening. The scene at the gym was described as chaotic, with shocked students and parents searching for each other in the crowd. If students could have been contacted easily at home, it would have been preferable to send them home once their parents had found them.

Polling responders is difficult

Organizing a large-scale disaster response requires knowing who is on site, who is on the way, and how many additional personnel have to be called up. This information is not always easy to obtain in an emergency.

Emergency Medical Services (EMS) coordinators could not establish, after the 9/11 attacks, exactly who had responded to calls for help and who was going to respond. The login procedure required a radio number, but some personnel arrived without their radios and were never logged in. Other EMS and ambulance personnel were not dispatched but arrived at the scene in response to a recall of all firefighters to the scene. In the end, EMS coordinators had to ask battalion headquarters to telephone the homes of all unaccounted-for personnel.

Inconsistent information is issued

“Miscommunication heightens during a crisis and can be exaggerated by half-truths, distortions, or negative perceptions,” concludes a report on the 1998 Florida wildfires. During this crisis, officials relied on media to tell the public what was occurring and how they could protect themselves. But local governments did not always centralize communications, and many reporters complained that other news organizations were receiving more information or better information than they were.

Similarly, the Centers for Disease Control (CDC), the United States government agency responsible for responding to the 2002 anthrax attacks, came under severe criticism for releasing incomplete and inconsistent information about the attacks. Local officials stated that they had to obtain information from the news media instead of from the CDC. Inconsistent communications can confuse the public about the degree of danger they are in and the precautions they need to take.
Incident Notification: Remedy for Communication Failures

Incident notification systems are specifically designed to address common communications failures, and many of the failures described above could have been mitigated had an incident notification system been part of the disaster response and recovery plan. Incident notification lets disaster coordinators take advantage of whatever communication pathways are open to deliver consistent messages quickly and keep a running tally of the responses to those messages.

Redundancy is one key to the success of notification solutions – not only are messages sent to a given recipient on multiple pathways, but the systems themselves are designed with multiple physical redundancies. For example, a vendor might lease dedicated phone lines from several different national carriers, and store identical customer contact information in multiple data centers thousands of miles apart. Although no system should be considered “fail-proof”, incident notification systems are not only efficient through saving time, but also offer a level of reliability and security a single system cannot match.

<table>
<thead>
<tr>
<th>Communication Failure</th>
<th>Incident Notification Remedy</th>
</tr>
</thead>
</table>
| Communication systems are damaged | Multiple communication networks and paths (not all channels will be damaged)  
Redundant, geo-dispersed systems can survive regional failures |
| Communication equipment isn’t functioning | Multiple notification paths (phone, cell, e-mail, fax, PDA, SMS, etc.) to circumvent single point of failure |
| Multiple agencies can’t communicate with each other | Telephone conference bridging can supplement the use of tactical UHF/VHF radios |
| The disaster coordinator’s location is inaccessible | Notification system and contact data are accessible from anywhere  
Administrator can delegate authority to an alternate whose office is intact |
| People aren’t where they were expected to be | Multiple communication pathways maximize chance of rapidly finding people |
| Contact information is out of date | Easy-to-use Web or phone interface encourages people to maintain their own data  
Automatic generation of requests to update contact information  
Automated testing of contact paths |
| One-on-one communication takes too long | Thousands of calls can be placed in a few minutes, and conference calls with key personnel can be initiated on the fly |
| Polling responders is difficult | Automated polling and real-time summaries of polling data |
| Inconsistent information is issued | Distribution of identical recorded or text messages allows accurate and consistent information flow |
Preventing Communication Failures

Clearly, not every communication failure can be averted. The scale of a disaster may be great enough to overwhelm any planning efforts. But in many of the real-life cases cited, incident notification in conjunction with effective planning would have saved lives and property, reassured the public, and gotten businesses and public services up and running much sooner.

Although an incident notification system can never guarantee complete success, certain features can make it as fail-safe as possible. To understand what these are, it’s helpful to consider all the steps a coordinator must take in order to communicate successfully during a disaster.

Initiating messages

The first task facing the disaster coordinator is to initiate messages. This can be a formidable challenge if the command center has been damaged or if communications lines are down. Incident notification simplifies the task by reducing the number of messages that must be initiated.

An incident notification system allows the coordinator to issue a single message to an entire list of people – whether that group consists of police SWAT team members, critical vendors, ambulance crew chiefs, parents of schoolchildren, hospital intake liaisons, or reporters. The chances of initiating messages successfully are much greater if the coordinator has to send only five messages instead of five thousand.

Fortunately, it’s rare for all communication links to fail at the same time. Even in the aftermath of the 2001 World Trade Center attack, when landline and cellular telephone services were severely compromised, Internet and text messaging services were largely unaffected.

The variety of communications media available today often makes people feel they can never really “get away from it all.” The benefit is that there is nearly always some way to contact the incident notification system.

For incident notification to be truly accessible in an emergency:

- There must be multiple ways to initiate a message. At the very least, disaster coordinators should be able to contact the notification service through the Internet and by telephone. They should not be required to be at a particular computer or a particular telephone to initiate a message. A single dedicated connection is particularly vulnerable to failure.

- There must be multiple ways to record and reformat messages. With an incident notification system, the message isn’t necessarily delivered in the same format that it’s received in. The message initiator should be able to dictate a message to an operator, record a voice message by telephone or Internet, or type a text message using the
Internet or a telephone text-messaging device. Live operators or system software should be able to convert text messages to speech and vice versa.

- The system must be able to accept messages from multiple initiators. Disaster coordinators should be able to delegate authority to several associates so notification won't fail if one person is incapacitated or unavailable.

- The system must have at least two widely separated physical locations, so that it won't become unavailable in the event of a region-wide disaster.

- The system should use redundant electrical power sources, communications carriers, and Internet service providers to minimize the chance that it will be put out of commission.

**Delivering messages**

After a message has been initiated, it must be delivered to everyone on the list. There are two important issues: whether the messages will arrive, and when they will arrive.

To maximize the likelihood that messages will be delivered:

- The notification system must be able to send messages to all types of contact devices – landline phone, wireless phone, fax, ISP-based email, BlackBerry (wireless email), pager, PDA, instant messenger, and more – and in as many formats as possible (voice, text, SMS).

- The system must permit unlimited contact numbers for each person on the list, and allow a different order for each list member. (For example, Member 1 might designate cell phone first, then email, then fax; Member 2 might designate work phone first, then home phone, then pager.)

- The system must be able to make unlimited attempts to contact each person on the list, until there is confirmation of receipt.

- Blanket geographical notifications should make use not only of 911 listings but also of any other white page or opt-in contact information for the residents of the affected area (in other words, geographic and contact-list data should be cross-referenced).

To deliver the messages as quickly as possible:

- The system must have adequate line capacity. With a sufficient number of lines, it is possible to deliver thousands of messages in just a few minutes.

- Telephone lines must be dedicated to the system, and not shared with other users who will be in contention for them.
Selecting the right people to notify

A well-designed incident notification system must be able to send messages to everyone who needs to be notified. In practice, this means that:

- There should be no limit on the number of list members allowed.
- Messages should be deliverable anywhere, including in foreign countries.

Nearly as important as reaching all the critical participants is sending messages only to those who need to receive them. Sending extraneous messages in times of emergency can have serious unintended consequences, including chaos and crowding at the disaster site, an influx of unwanted phone calls, and even mass panic. To filter messages correctly,

- Unlimited lists and sublists must be allowed. The disaster coordinator may need to poll employees from the seventh floor to make sure they were all safely evacuated from the fire on that floor; instruct employees in the Network Services division to report to the backup site the next morning; or recall some ambulance crews but not others.
- Relationships between list members must be tracked. This allows the disaster coordinator to make selections based on the relationships – for example, contacting all parents of sixth-graders.
- Geographic notification, which is used for evacuating neighborhoods or warning people of potential dangers, must be fine-tunable. For example, the residents of the blocks closest to a fire might be told to leave immediately, while those a few blocks farther away might be told to prepare for evacuation.

Maintaining accurate contact lists

With or without incident notification, one of the primary responsibilities of a disaster coordinator is maintaining accurate contact lists. An incident notification system can help protect data integrity if it is well designed and administered.

- There must be a facility to upload existing contact lists. If a list has already been created and vetted by the organization, re-entering data would run the risk of introducing errors.
- List members should be able to update their own contact information, including their contact path preferences. People are more likely to update their own information correctly, if only because it's easier for them to spot mistakes.
- Data must be properly secured. This requires using appropriate security software and developing and implementing adequate security procedures.
• List members must have confidence that the system administrators will protect their privacy, and will not release their contact information to any third parties. Ideally, systems should include an option to conceal personal contact information from administrators.

Receiving messages

Communication flows in two directions. Usually, sending out messages isn't enough. The disaster coordinator must find out who has been contacted successfully, and, sometimes, what their responses are. With direct, one-on-one communication, getting an answer isn't usually an issue (although it may be if the caller has to leave a message). An incident notification system, on the other hand, needs a mechanism to receive and report responses.

To facilitate two-way communication:

• The system must be able to receive a response such as a touch-tone signal to confirm that a message has been delivered successfully.

• The system must be able to receive multiple responses such as touch-tone signals to answer questions posed by the original message. For example, if first responders are being notified, the coordinator's message might ask them to press 1 if they are already at the disaster site, press 2 if they are on their way there, and press 3 if they are unavailable to respond to the emergency.

• Real-time reports of all message delivery attempts, confirmations, and polling results must be easily available by Internet, fax, and email. Both summary and detail reports are necessary. Summary reports can quickly communicate the overall picture – how many recipients have been reached, how many are on their way, and so forth. Detail reports can show where individual follow-up is needed. For example, in a neighborhood evacuation, rescue personnel can focus their efforts on the houses where residents indicated that they needed help.

Performing other critical tasks

Disaster coordinators have other tasks besides sending and receiving messages. But as we have seen, one-on-one communications are so time-consuming under the best of circumstances that they can delay recovery and even lead to loss of life. When other communications failures are added to the equation, coordinators may end up by being preoccupied almost exclusively with communications.

Any functioning incident notification system will greatly reduce time spent on communications and will free emergency personnel to deal with rescue and recovery work. Being able to initiate a few messages and receive hundreds or thousands of responses formatted in a readable report a few minutes later is an enormous time-saver.
In addition, a well-designed notification system will have several features that are specifically geared toward making emergency personnel more effective.

- Conference bridging allows real-time communication among some or all members of a list – in effect, spontaneous conference calls. Conference bridging can be used when the return message is more complicated than “I'm on my way.” It can enable coordinators to start planning even before they reach the emergency command center, and under some circumstances it could supplement radio communications at a disaster site.

- The ability to create and store messages in a library before a disaster even occurs means that coordinators can begin the rescue and recovery process simply by clicking on a button.

- The ability to store messages for scheduled release allows disaster coordinators to create a series of messages in a single sitting. This not only saves time in creation but also reduces their risk of being unavailable to initiate follow-up messages.

- Finally, the system should be easy to use and should not require extensive training. Just as coordinators should not be spending hours making phone calls, they should not be trying to remember complicated command sequences or searching for user manuals.
About Everbridge

Everbridge, the world’s recognized leader in incident notification systems, merges technology with industry expertise to help millions of people communicate in a crisis and connect on a daily basis. The company’s notification platform and incident lifecycle communications model make communicating to many as simple and effective as communicating to one. Organizations in more than 100 countries—including Salesforce.com, AirTran Airways, the American Red Cross, and Virginia Tech—rely on Everbridge for their emergency notification and day-to-day incident communication needs. For more information about Everbridge, visit www.everbridge.com.

Contact Us

Everbridge
technology + expertise

888-366-4911
www.everbridge.com