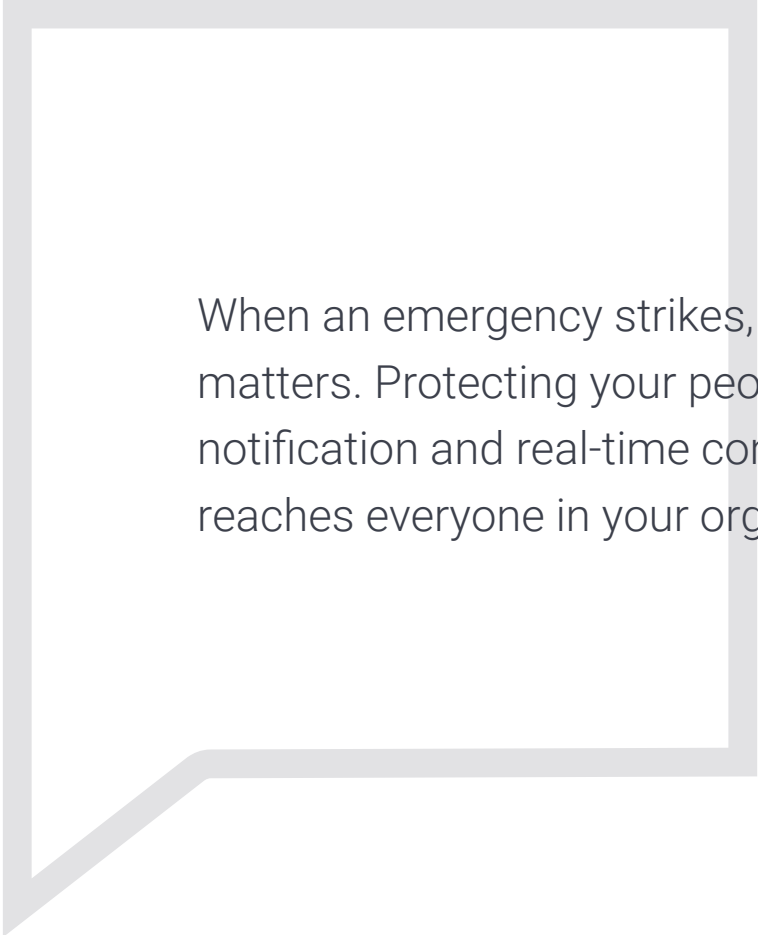**Af** | AlertFind

THE RIGHT COMMUNICATION AT THE RIGHT TIME

Emergency Communications
And Alert Strategies

20
18

When an emergency strikes, every second matters. Protecting your people requires rapid notification and real-time communication that reaches everyone in your organization.

This communications planning is a key part of your emergency preparedness plan. Think of this plan as your toolkit. By having all of the right tools at your disposal in this toolkit, you'll be better prepared for any situations you face.

Emergencies cause chaos and panic, whether it's an active shooter event, a natural disaster or another crisis. That's why your organization needs a clearly-defined plan, created with the input of the right stakeholders.

BUILDING YOUR COMMUNICATION STRATEGY AND EMERGENCY ALERT TOOLKIT
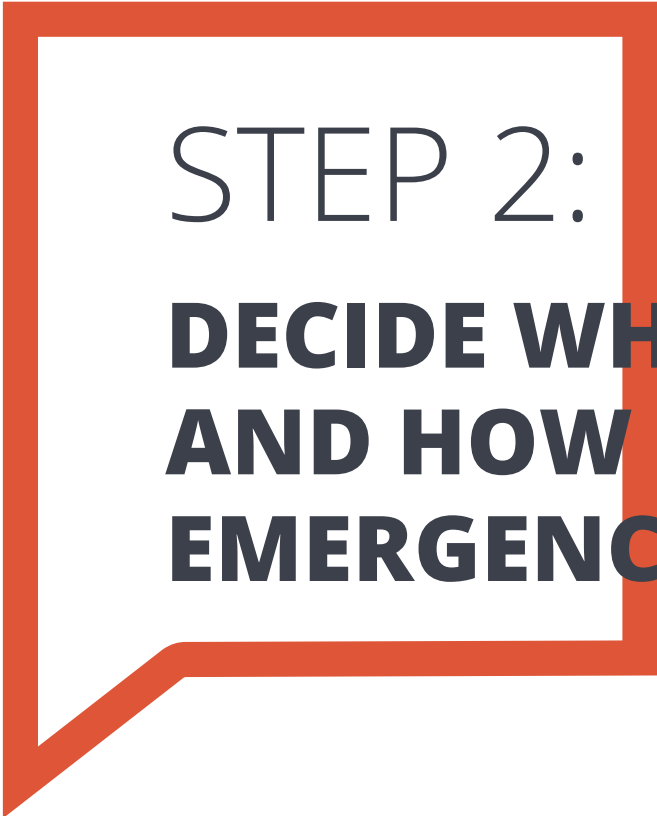
STEP 1:

BRING TOGETHER THE RIGHT PEOPLE

When starting your emergency preparedness planning process, bring together all of the right stakeholders. This should include your emergency management team, communications team and any other relevant people in your organization. Depending on the hazards you face, this could include facilities management, IT or other departments.

Your human resources (HR) department should have a key role in planning because they play a critical role when dealing with the aftermath of an emergency.

For example, which employees will be asked to work from home? Which ones will need additional support after the emergency? Perhaps most importantly, emergency management teams may need access to contact information for employees and their families in the event of a death. Most emergency management programs don't have this information, but HR does.

When building your toolkit, remind HR about the importance of regularly collecting contact information and other critical data from employees or use an emergency notification system that automatically updates it for you. Keeping the employee database up-to-date helps you provide real-time notifications to every employee during an emergency and manage the aftermath.

As you're planning, always remember that emergency preparedness planning won't work in a vacuum. You have to engage all of your stakeholders to build a comprehensive toolkit and avoid any gaps in your emergency response. The middle of an emergency is not the time to find you don't have the right contacts or information to move forward.

STEP 2:

DECIDE WHEN AND HOW TO SEND EMERGENCY ALERTS

With your group of stakeholders, do a threat assessment to determine what threats and hazards the organization faces. Then start to develop potential messages that could address each specific risk.

Using an Excel spreadsheet, create an outline for your threat assessment and the associated actions. List your top 10-20 risks in the left-hand column, and across the top list all possible emergency management actions you'll need to take.

For example, risks might include:

Active shooter

Hurricanes

Mudslides

Server failure

Power outage

Security breach

Your emergency management actions might include:

Activate your Emergency Operations Center

Alert the entire organization

Send an alert to senior leadership

Lock down the building

Activate your remote working plan

Give each risk a severity level, and put a checkmark to designate the relevant action for each threat. You can use this grid as the framework for your emergency preparedness plans.

Here are some specific examples of threats and actions by department:

IT

Threat:

Your email goes down and you want to send an outage notification, but it's usually done via email.

Action:

Use an emergency notification system that provides multi-channel alerts, including email, text, voice call, fax and mobile app push notifications. IT is the lifeblood of any organization, so you want to have a variety of communication options and emergency communications strategies for when the internet goes down.

FACILITIES

Threat:

Your building experiences a functional problem, such as a water main break, power outage, chemical spill or loss of heat.

Action:

Send an alert to all employees who work in the building instructing them to avoid the area, leave the building or go to another facility.

CYBERSECURITY

Threat:

A data breach takes place or one of your systems is hacked.

Action:

Immediately notify people about the breach and advise them to take protective steps, such as logging out of the system.

STEP 3:

PRE-SCRIPT YOUR ALERTS

The key is to not wait until you're in an emergency to craft your alerts. Your emergency management team should script messages in advance for all hazards you identify.

When scripting emergency alerts, think about whether you can include a link to a reputable site for more information. For weather alerts, you can use ready. gov. Managed by the Department of Homeland Security, the site will tell people what to do before, during and after any weather event, and also can provide more information to prepare.

Use these links when building your templates or pre-scripted alerts. This ensures the information always stays at the bottom of the message.

As you script your alerts, think about audience, message and mode:

AUDIENCE:

Who is the alert going to? With an emergency notification system featuring in-app GPS check-ins, you can target only those people affected by a location-based event.

MESSAGE:

What should the alert say? Your message is designed to help protect people, so it should be short with easy-to-understand language.

MODE:

What channels are you going to use? It's best to have the option to send messages across multiple channels, from email and text to mobile app push notifications and pagers.

You'll also want to make sure your alerts are answering these three questions:

1) What is the hazard?
2) Where is the hazard located?
3) What protective actions do you want people to take?

Be clear and concise in your message. Otherwise, you'll be creating more problems than you're solving.

As an example, imagine a chemical spill happens at your office park. Your alert to all employees might look like this: Chemical spill by the Northside Buildings. Quad Road is closed. Use Lake Drive to access Buildings 103 and 104.

When alerting your emergency management team, you want to:

IDENTIFY YOURSELF: Be clear that the alert is coming from an official source. For instance: This is the [company name] Emergency Management Department. We have a [facilities/security/cyber/IT-related] situation that requires your attention. Press 1 to dial into a conference call.

STAY CALM: Try to avoid creating panic. Calmly brief the team on the conference line about the situation.

NOTIFY THE BROADER AUDIENCE: Use your emergency notification system to alert your employees.

STEP 4:
CAREFULLY REVIEW YOUR ALERT COPY

When pre-scripting alerts, it's easy to get caught up in worrying about your organization's reputation and image. The desire to craft a message in a particular way often leads to making it too complicated.

Write alerts using plain language that your audience will understand. Avoid using jargon or technical terms that only public safety and IT officials might understand. You want to clearly state the threat and the actions you're asking people to take.

The best alerts are brief and stick to the facts. *Remember, your goal is to get the necessary information out to people so they can react quickly and stay safe.*

With that in mind, it's important to strike a balance between issuing an emergency alert quickly and making sure you're prepared with the right information. Take a minute to fully understand the scope of the incident and gather all of the facts. You don't want to rush to release an alert and further confuse people in an already scary situation.

STEP 5:

DO TESTING AND TRAINING AHEAD OF TIME

Proper preparation and training helps ensure that everyone in your organization is ready to act reflexively during an emergency.

For example, when developing an active shooter preparedness plan, your training should include the Avoid, Deny, Defend plan created by the ALERTT Center at the University of Texas:

AVOID THE SHOOTER: Identify alternative exits so people can flee the scene as safely, quickly and quietly as possible. Make sure people are familiar with floor layout plans and/or escape routes in any buildings they spend a lot of time in.

DENY ACCESS TO THE LOCATION: Establish interior shelters in case people can't leave the building safely. Rooms with an interior, locked, commercial door provide the best protection. Other good places to shelter include a closet, office, bathroom or any other room that has a commercial grade locked door with no windows.

DEFEND YOURSELF; attack in groups: Launching an unexpected counterattack can save lives. Train people to look around their surroundings for an improvised weapon, such as coffee pots, scissors, canned food or heavy objects.

Training needs to extend beyond active shooter situations. Think about all of the threats you identified in your original threat assessment and use those areas to do training.

It's also important to regularly test your emergency notification system. A good way to test it is during an evacuation drill. You're already disrupting the organization, so it's an ideal time to send a test alert to everyone.

If your organization uses an emergency management system with a notification opt-in that people sign up for, this is a great way to build awareness. When some people get the test alert and others don't, those in the latter group will want to know why they didn't receive an alert. Then you can easily get them to sign up for emergency notification system.

STEP 6:

PREPARE FOR POST-EMERGENCY CHALLENGES

You can plan and train, but until an emergency situation occurs, you don't know how people will react. Everybody reacts differently to a crisis.

Some people will also feel the effects long after the event, so you should work closely with HR during planning to create a list of support services and actions.

For instance, following an active shooter event, many people don't want to return to the office or building where the shooting occurred. You'll have to make decisions about whether to close that location or offer people the opportunity to work at a different building.

As you're building your emergency preparedness plan, don't forget to think about what you'll do after the emergency situation is over - whether it's offer individual counseling, remote working or a transfer to another location.

BUILD YOUR EMERGENCY ALERT TOOLKIT NOW TO BE PREPARED

Building your toolkit requires thinking critically about your organization and the threats it faces. Everyone who is involved in managing those threats needs to have a role in the planning process.

With the toolbox approach, each person and department becomes a part of your emergency preparedness plan. When an emergency calls for them, they're available to help you and you have already built a working relationship with each one. Whether it's facilities, compliance, police, fire, public works or IT, all of those different resources are in your toolbox, ready for you to draw them out depending on the incident.

That's why you want to build as many relationships in advance of an emergency event as possible. Doing so better prepares you for when an incident happens and helps you respond more effectively.

During an emergency, you don't have time to plan. You need to be able to react quickly, whether you're facing an IT problem, a natural disaster or an active shooter event. Building a comprehensive plan in advance with pre-scripted alerts is the best way to make sure you're ready to help protect your organization.

Need some expert insights to improve your emergency preparedness planning?

Take our online assessment and get tactical advice to improve each area from emergency preparedness expert Bob Clark.

TAKE THE ASSESSMENT

Af | AlertFind