



Seven Deadly Sins of Emergency Notification

Unfortunately, crisis happens. Recently, all too often.

Many companies are not fully prepared to communicate rapidly and effectively in a crisis. This article covers the common mistakes all business continuity and disaster recovery professionals should avoid to avert disaster and foster resiliency.



ONE:

Failing to make users aware of your crisis communication method or system.

A good example of this is the use of email for non-routine alerts. The increasing threat of phishing emails and hackers means your user base has a healthy mistrust of unfamiliar messages.

In fact, your IT Department may spend significant time educating employees on the dangers of suspicious emails. Staff may be encouraged to only open emails from known senders. So if you send an emergency alert from an email account that they have never seen before, they might delete it without ever seeing the content.

When you send an emergency alert through your notification system, make sure it allows you to enter a “From” email address for the message. Then, where possible, use the same email address consistently across your notifications. Make sure this address is in your company’s address book so that the alert will not appear to come from an unknown sender.

Also consider standardizing at least a portion of your subject line to include identification of the notice as an urgent message (e.g., “Company XYZ Emergency Alert”).

TWO:

Using outdated contact information.

Regardless of how reliable your notification system is or how quickly you send an alert, if you don’t have the correct contact information, your message won’t be conveyed.

Be sure you have a fail-safe method of updating contact information; ideally through a contact database integration or by using your notification service’s self-registration/update feature.

THREE:

Not considering the diverse nature of a global workforce in your plans.

Don’t overlook the fact that your message recipients may speak different languages. Notification systems that provide for multilingual messaging are invaluable in a global environment. As part of your alert enrollment process, be sure to ask your contacts for their language preference so that alerts are automatically and consistently translated for them.

Also keep in mind that if you are sending messages internationally, you may have to deal with a cultural distrust of automated calls. If this is the case you’ll want to work with local management to ensure individuals are informed about the critical reasons you are using an automated system to send alerts.

FOUR:

Excluding travelers and mobile workforce.

Travel is part of almost every large corporation making it difficult to know who is impacted by an incident in a particular city or location. While traditional alerting methods (i.e., email, SMS, voice calls) are essential and relevant, many organizations also need secure and resilient communication to target their “on-the-go” mobile workforce.

Consider notification providers that support alert initiation based on geographic position —be that the location on record in your contact database (e.g., home address or office address) or the GPS location of their smartphone.

This ensures that anyone in the vicinity of a crisis situation will be alerted even if their travel itinerary isn’t on file.

FIVE:

Failing to consider digital security.

It goes without saying that in today’s data-centric world one of the most important considerations for choosing a notification provider should be data security.

Never choose a provider that cannot explain, in detail, the measures they take to ensure your account is secured against attacks, system failures and loss.

Involve the digital security experts in your organization when reviewing vendors to help determine that the platform is secure, reliable and resilient. They may be best qualified to evaluate the certifications and features of systems in order to ensure that your data will never be compromised.

SIX:

Assuming everything goes as planned.

As Benjamin Franklin is quoted as saying, "by failing to prepare, you are preparing to fail". In no context is that truer than in business continuity.

A critical component of any good plan is communication and that includes a reliable notification system.

Notification systems are not only important during a crisis, they are also invaluable afterwards for:

- Communicating alternative work sites
- Confirming who is available to work, who needs an alternate work site (requires a notification service with two-way communication)

- Providing frequent updates
- Having a common repository for important documents that employees can access and share even if your network is down. Make sure your notification tool provides this lock-box feature where these documents can be stored and retrieved.

SEVEN:

Using complex communications processes.

There are a lot of potential pitfalls in crisis communication. Here are a couple that we see most frequently.

The first is having a complex accountability structure for employees and temporary staff. This often includes communicating with phone chains or trees that can break down easily. Every organization can benefit from a simplified plan to contact the masses as soon as possible using simple, reliable notification technology.

Those organizations that do have a notification system in place often make the mistake of only having one or two employees authorized and trained to send alerts. Communication can be significantly delayed or break down altogether if those individuals are not available, or are not well-informed of the situation and able to provide direction. It's important to give rights to activate messages to multiple individuals, ideally from different areas of the company.



While crisis may sometimes be unavoidable, business disruptions and loss don't have to be. Avoid these Seven Deadly Sins and lead your organization through dark times to come out as a stronger, wiser force for good.

For more information: onsolve.com // 866 939 0911

