ENS TESTING BEST PRACTICES

It is up to you to decide how to best test your emergency notification system (ENS), since no two organizations are exactly the same. Taking a look at how other organizations test their systems, however, is quite helpful when making policy decisions.

WHY TEST?

Testing the ability of your systems and infrastructure to effectively handle the high volume of traffic that an emergency situation generates is important. Compare your Emergency Response strategy to a fire drill; you're not just measuring how fast the word gets out, you are also making sure that the people recognize what the siren means and are prepared to take the appropriate action. Testing also allows you the opportunity to document and analyze the success of each notification method to better understand the most effective methods for communicating with your population.

Having a scheduled and documented testing plan helps guarantee that, in the event on an actual emergency, your population will receive the message and respond to it appropriately. Testing your emergency plan will help keep you sharp when a real emergency occurs and gives you the opportunity to troubleshoot any problems that may occur before a possible life or death situation arises. Testing is also a chance to raise awareness of how an alert will appear to a recipient, and potentially increase participation / enrollment.

HOW OFTEN DO YOU TEST?

When trying to decide whether a plan is best for your organization, it's often valuable to compare practices. We took a random polling of the Omnilert administrator community and compiled the results to look for some true "best practices."

A brief survey was sent out to a random sampling of Omnilert clients asking about some basic testing practices. The first 100 organizations to respond provided the results, and some trends were very easy to spot.

The vast majority (82%) of organizations polled do test their ENS regularly. Of the 18% of organizations that do not test, half of them expressed an interest in a testing procedure, but simply do not have the time or resources to put a plan together at this time.

Forty-four percent (44%) of the total polled test twice a year, with a smaller amount (14%) testing once per month. Some organizations polled (16%) have a testing plan in place, but test "as needed," rather than on a schedule.

A full sixty-two percent (62%) perform a "full test" during the year, sending SMS and emails to all users, rather than a limited "test list." Of those, 8% perform additional testing at other times during the year, but send messages to a limited testing group, instead.

ANALYZING THE RESULTS

For the most part, the criteria for a successful test differed from organization to organization. Most also differ in how they respond to their testing results. Many of the administrators stated that they do not review the results in any way, and simply leave it up to their population to verify that they received the message. Several also stated that the email and SMS tools "simply work," so there is no need to review the results.

Other organizations simply look for a successful send as their testing "goal," and if the message appears on all of their endpoints... posting to Twitter or Facebook, appearing on their website or digital signage, or setting off the sirens... then they consider the test a success.

Of those that do use delivery statistics to analyze the results, testing is usually followed by a questionnaire, or mass email requesting that the "failed" users modify their account settings or contact a support department for assistance.

TO TEST OR NOT TO TEST?

Testing your emergency plan will help keep your team's skills sharp and allows you to troubleshoot any problems before an actual emergency occurs. Keep in mind, it's not just about testing your emergency notification system, it's also about testing your infrastructure and connected devices, your internal team and processes, as well as managing your population's expectations for your notification system.

HOW MUCH IS TOO MUCH?

When it comes to testing your ENS, some people think of text messaging only, but other methods of communication built into your system require regular attention as well.

You may also send messages to your users via opt-in email or S.E.E.D. Many organizations also use emergency notification systems to send messages to social networking sites such as Twitter and Facebook, or to their own web pages. Testing this functionality and the response that it elicits is important as well. If you push messaging to physical devices, such as PC desktops, loudspeakers or digital signage, you'll want to verify that those connections are still configured properly, and that your community recognizes that emergency messaging may/will appear there.

Testing is as much about preparing your community for an emergency and how they should recognize an emergency situation as it is about testing your ENS. We advise that you perform a "full test" to all of your users regularly, but no more than 3-4 times per year. Sending a full test about twice a year seems to be the "sweet spot" for testing.

Overuse of test broadcasts, especially to your text messaging users, has the serious potential to lessen the impact of the system in an actual emergency. A perfect example of this is the car alarm. If your car alarm goes off every night for a week, your neighbors just start to ignore it or even demand that you turn it off,

More than a few tests a year to your full user-base could lead to people ignoring real threats or seeing your alert messages as SPAM, and unsubscribing altogether. It's important to balance the benefit of your system tests versus the possible backlash.

WHAT TO EXPECT FROM YOUR TEST RESULTS

Now that you've completed your test, what's next? After your tests have been performed, it's important to review your results. You can use your emergency notification system's built in delivery reporting, and/or send out posttest surveys, or simply review feedback left by email. But how do you gauge success or failure? How many of your text messages,emails, etc. should be delivered? Why are there some failed deliveries?

Obviously, with any mass communication, some messages just won't get through. People change their e-mail address, go over their mail quota, etc. Some cell phones will be out of range, have changed carriers, or canceled texting altogether. In a system test you should expect to see some emails and texts rejected. That's why your tests should include all of your endpoints in your alerts. The more communication channels you use, the more likely a user is to get the message.

The key to interpreting your results is to look for trends. If the same mobile carrier always seems to reject texts, it may indicate a problem in your area that can be addressed. If a large number of emails on your organization's domain show up as rejected, you may need to double check your local rewall or spam filter. If a large number of voice calls show up as "busy", you may be overwhelming your local phone lines. Your delivery status and user feedback can help you troubleshoot all of these situations.

In a general sense, if delivery (text, email, or voice calls) is above 90% success (Accepted, Delivered, etc), your stats are in the normal range. In many of our case studies, we've seen texting success rates of 95% or higher, which is outstanding for any mass communication on any medium.

TRAINING

System tests are also a great time to review your emergency guidelines with your administrators before an emergency happens. They may know how to initiate a message, but do they know when to use it? Do they know what to type and which group(s) to select? What triggers an Administrator further down the chain of command to issue an alert? Regular refresher training makes sure that your team knows what to do when a real emergency occurs.

About Omnilert

At Omnilert, we believe no one should ever die or get seriously injured due to lack of timely and accurate information. Our suite of emergency notification and critical communication solutions empowers organizations to keep their people informed and their operations viable during the most challenging times. We transform the way those responsible communicate with their people to rapidly disseminate critical information, automate emergency communications, accelerate emergency response, ensure business continuity, and recover quickly from a crisis. Our people and technology, together, help ensure successful outcomes for our customers.

OMNILERT | 202 Church Street, Suite 100, Leesburg, VA 20175 | 800-256-9264 | omnilert.com