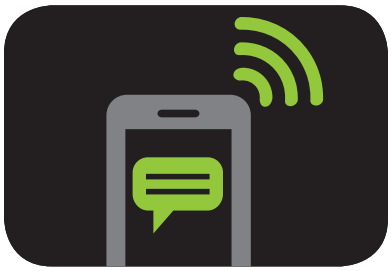
omnilert®

WHITE PAPER

7 Steps to Selecting an Emergency Notification Provider

In today's market, the term 'Emergency Notification' has become somewhat ubiquitous. Emergency notification providers run the gamut from full crisis communications platforms, working closely with cloud computing giants to provide top notch service, to mom-and-pop operations running off of ten-year-old desktop computers in a garage somewhere. Research in the market shows that features, functionality, price, and experience can vary wildly.

Not all emergency notification systems (ENS) are created equally. It's important to consider many factors when choosing a vendor and make sure that your emergency service isn't a dud. In our experience, we've found that there are seven key factors to ensure successful crisis communications and the right crisis communications provider.



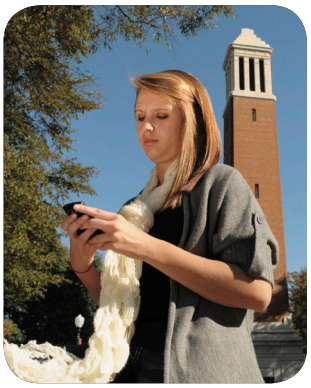
1 Understand How SMS Messages Are Sent

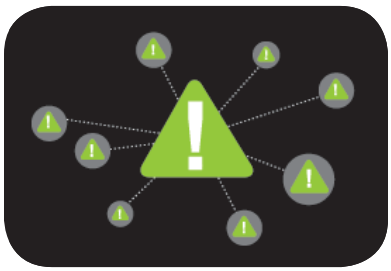
The fastest and most popular means to contact your people is usually SMS/text messaging. We know that over 90% of American adults own cell phones and 58% own smart phones. In an optimal setting, a Tier 1 Notification provider can deliver as many as 48,000 SMS text messages in under a minute.

Message delivery speed is an important factor to consider when selecting an emergency notification system. To understand how fast a message can reach your community, it is vital to understand the differences between the technologies used to transmit SMS messages.

Does your vendor send messages via short code or email? Sending text messages via email can significantly delay delivery. If you send a large number of messages, they may even be blocked completely by the mobile phone carrier as “spam.”

Short code SMS is fast, distinct, universally accepted, and secure. However you should know if your vendor uses a dedicated short code or a “shared” short code. A “shared” short code allows multiple services to use the same phone numbers. The same phone number that sends your emergency alerts could be used to sell ringtones, ads, or anything else. Email SMS transmission and shared codes lower the operating costs for vendors, but can compromise the integrity of your alert services.





2 Embrace Multiple Modality

At any given time, some of your community will likely be unreachable by text message. By expanding your reach beyond SMS, you increase your coverage by including web pages, social media sites, rss readers, digital signage, outdoor warning systems, desktops, and more. Most organizations benefit from unified emergency notification systems, not a bare bones mass text messaging systems. Be sure to consider services that will deliver a notification to your entire community all at once, by all means necessary to increase the odds that individuals receive your message in a timely manner.

Many organizations simply do not consider multimodal communication because they believe it to be beyond their reach, either too difficult to implement or too expensive. In truth, you should be able to extend your unified notification methods beyond text messaging and email with just a few relatively simple steps.

3 Consider a Hosted System

Why should your your ENS be available online or off-site? Simply put, hosted solutions are more reliable, more secure, and generally less expensive than their locally installed counterparts. Very few institutions have data centers designed from the ground up to run and protect mission-critical servers.

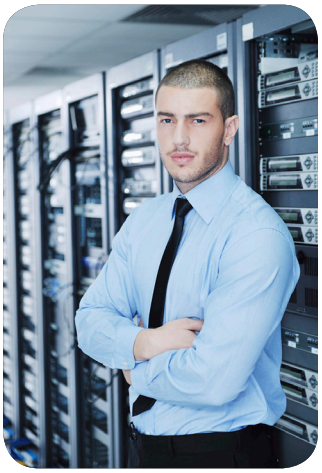
Hosted service providers have personnel and procedures in place to deal with any problems on the application end, usually with no interruption in service for you. Do you have fire protection, biometric security, 24/7 monitoring, and redundant Internet connections? Can you automatically switch to an alternate data center if power is disrupted locally in a disaster?

Do you have a full-time systems administrator that keeps up on the latest software patches and upgrades your systems on a continuous basis? Loss in data can prove costly for a company. It is therefore essential to have a process that regularly backups your data, keeps its secure, and preserves its integrity. With managed services, you as a business owner can have the peace of mind that your data is secure and backed-up because your hosting provider has process and procedures in place to deal with such scenarios.

Purchasing, maintaining, and upgrading your own hardware and software can be very expensive. Compared to the cost of a subscription service, it quickly becomes apparent that a managed solution is much less expensive. With a hosted service, you gain the peace of mind that your data and applications are secure and safe.

4 Ensure Privacy and Data Security

Server security is a primary priority for any business. It emcompasses various aspects of security: running security audits, spam filtering, virus scanning, software firewall configuration, OS updates, and much more. Your provider should be well equipped with various tools and extensive experience twith server security related issues.

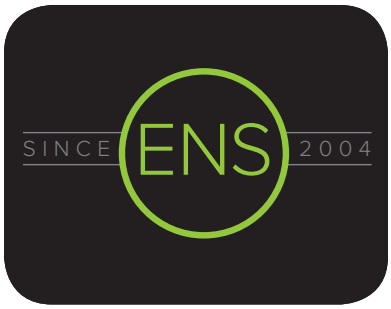


Remember that your ENS will contain personal contact information for all of your employees/ community. What will your vendor do with that data? Will it be shared? Carefully review your provider's terms of service, or the terms of use that they display to your subscribers to make sure that your data will not be used without your permission.

5 Demand Professional Services and Customer Support

How well will your vendor support you and your notification needs? Emergency communication products should be easy to use but what about setting them up? Make sure your provider offers training for you and your staff. Not only should they be able to train you on how to use the software, but should also address questions, and share best practices for actually using the system.

A solid emergency notification strategy always includes a plan for improvement. Regular test results should be available to you so that you cannot just check your delivery rates, but also review your coverage and see if your current end-points are truly meeting your needs. Ideally, your provider has a dedicated account staff to help you analyze the results and recommend improvements.



6 Confirm Experience and Longevity in Critical Notification Services

No one wants to be the 'test' client, especially when it comes to crisis services. Be sure that any provider that you choose is fully invested in crisis communication. ENS services, as an industry, is still booming and many companies are starting up looking to grab a piece of that business. Make sure that any vendor that you choose has experience in emergency communications, not just mass communications. A company that excels at mass marketing may not know the ins and outs of crisis services. It's important to know where your potential provider came from, not just where they're going.

7 Enjoy Ease of Use

A well-designed ENS should be simple to use, so that in a time of crises you and/or your staff can easily get the word out. Sure, bells and whistles are nice, but adding too many features to a system can take away from its core purpose: to allow you to get a message out quickly when seconds count. The easier a system is to use, the quicker you can get that message out to your population with confidence.

Conclusion

At the end of the day, it's important to remember that not all emergency notification systems are created equally. Emergency notification is a mission critical process, and properly vetting your ENS provider and communications practices are key factors in successful crisis communications.

Request a Demo

Learn how Omnilert's critical communication system can help keep your team safe and connected.

Visit www.omnilert.com
or email us at info@omnilert.com.

Omnilert, LLC invented the world's first campus emergency notification system and now supports all industries to keep people safe and connected. Their award-winning flagship service enables a single person to communicate critical information with thousands of people anywhere, anytime, on any device or service. This affords better crisis communications, emergency management, business continuity, disaster recovery, and crime solving. The company's 20,000 clients include the U.S. Army, Bayer, DuPont, Mazda, Philips, University of Virginia, CalPoly, YMCA, and American Red Cross. Omnilert solutions are sold under the brand names Amerilert, e2Campus and RainedOut. The privately held company is headquartered in Leesburg, VA., and at www.omnilert.com online.

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