

EXPERT ADVICE

How to Avoid Sending a False Alarm



The January 13, 2018 ballistic missile false alarm sent out to the residents and tourist population of Hawaii.

The ballistic missile False Alarm alert that occurred in Hawaii recently has underscored the critical role that these systems play in keeping the public informed. At the same time, it is leading many organizations to ask:

- + Could a false alarm happen to us?
- + What precautions should I take?

What went wrong that caused the Hawaii false alarm?

1. On January 13, 2018 a ballistic missile alert announcing an immediate threat was sent out to the residents and tourist population of Hawaii via both the Wireless Emergency Alert (WEA) and the Emergency Alert System (EAS) networks.
2. The alert was distributed to multiple communication channels, including television, radio, and cellphones in Hawaii. According to officials and multiple reports, the false missile alert was caused by a combination of human error and system design.




The underlying design of the actual emergency management system used makes a big difference in addressing this type of situation and avoiding false alarms like the one in Hawaii. To dramatically lower the risk that a wrong message would be accidentally sent broadly over Wireless Emergency Alert (WEA) or the Emergency Alert System (EAS) networks, we recommend using a Critical Event Management solution that's designed to with integrated controls and safeguards.

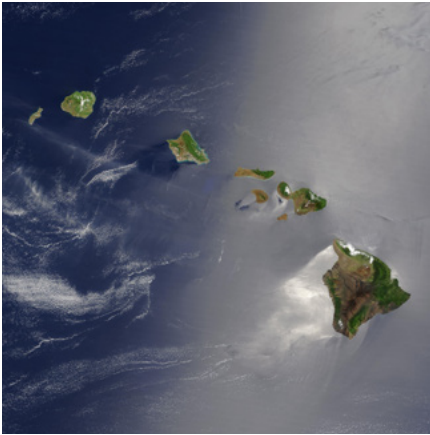
Emergency notification system critical features

1. **Distinct Test and Live mode environments** for sending messages via EAS or WEA. The system defaults to Test mode and the sender needs to proactively switch to Live mode to send out a message broadly.
2. **Access controls** so the administrator can establish exactly who has permission to send out a message over WEA or EAS.
3. To send out messages via IPAWS channels, including WEA and EAS, a user needs to enter IPAWS credentials each time, and not store any IPAWS credentials in the system. In conjunction with the need to have System Administrator credentials to log in, this provides a **two-factor authentication** requirement that makes it far less likely that someone without the proper authorizations can get into the system and send out messages.



ENS critical features

-  Live vs. Test Mode
-  Access controls
-  Two-factor authentication



It took 38 minutes to send out a correcting message announcing that the missile alert was a false alarm.

These three elements combined – distinct Live vs. Test Mode, Access Controls providing authorization, and the requirement to enter specific IPAWS credentials – dramatically reduce the likelihood someone would accidentally send out a Test message to a Live audience. Published stories indicate that several, if not all, of these elements were not in place in the system used in Hawaii.

Another area of controversy has been the 38 minutes it took to send out a correcting message announcing that it was a false alarm. Some articles have suggested 25 minutes of the delay was related to securing proper authorizations to send out the new message. In our experience, sometimes lags in authorization are due to lack of clarity on process and sometimes they are due to trouble locating the authorized party. A best practice is to pre-determine how to authorize a corrected message and who must be involved. Our system also includes a scheduling function to know who is on duty, who to escalate to, and how to reach all of the parties.

Advanced preparation can help with getting corrected messages out quickly—pre-defined notification templates can enable standard processes to be quickly followed. The Everbridge system includes a “Follow Up” option, which enables customers to Update or Cancel IPAWS-initiated alerts. It’s also important for alert initiators to conduct practice training drills in a test environment on an ongoing basis. Simulating circumstances forcing practitioners to respond both quickly and accurately will better prepare them for live situations and will ensure they know the system well.

Everbridge provides an IPAWS on-line training module in the Everbridge University Portal, which is available to all customers. This enables the user of IPAWS to understand all of the concepts and the usage of the system. The course is followed by an Everbridge certification test.

Although the Hawaii false alarm was not caused by a hack into the system, the incident has raised this topic as well. The Everbridge platform continues to undergo stringent security reviews by many of the largest and most rigorous companies in the world, as well as by State security teams, which are included among our 3500+ enterprise customers. The Everbridge Suite is FISMA (Federal Information Security Management Act) compliant, meeting over 250 controls mandated by our over 40 Federal agency customers, and we are implementing 75 additional controls to satisfy FedRamp compliance standards.

We know our customers have the extraordinarily important responsibility of keeping their constituencies safe and informed, and there is a lot of complexity to reliably and continually accomplishing this objective. A delicate balance must be struck: the underlying systems and processes must have safeguards, the right authorizations, and be secure; at the same time, they also have to be nimble so information and instructions get out quickly. We keep learning from our work with our customers to help us ensure that our software strikes the right balance and incorporates best practices. We are excited to continue this journey together.

To learn how the Everbridge Critical Event Management Platform is purpose-built to provide reliability and performance in all situations, visit everbridge.com.

About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise software applications that automate and accelerate organizations' operational response to critical events in order to keep people safe and businesses running faster. Every day, over 3,500 global clients rely on the company's SaaS-based Critical Event Management delivery platform to quickly and reliably assess the severity of critical events, locate the first responders, the impacted people and assets, automate the communications, collaboration and orchestration for faster incident resolution. The company's platform sent over 2 billion messages in 2017, and offers the ability to reach more than 200 countries and territories with secure delivery via over 100 different communication channels. The company's applications include Mass Notification, Safety Connection™, IT Alerting, Visual Command Center®, Crisis Commander®, Community Engagement™ and Secure Messaging. Everbridge serves 9 of the 10 largest U.S. cities, 8 of the 10 largest U.S.-based investment banks, all four of the largest global accounting firms, all 25 of the 25 busiest North American airports, six of the 10 largest global consulting firms, six of the 10 largest global auto makers, four of the 10 largest U.S.-based health care providers and four of the 10 largest U.S.-based health insurers. Everbridge is based in Boston and Los Angeles with additional offices in San Francisco, Lansing, Orlando, Beijing, London and Stockholm. For more information, visit www.everbridge.com, read the company blog, and follow on Twitter and Facebook.



VISIT WWW.EVERBRIDGE.COM

CALL +1-818-230-9700