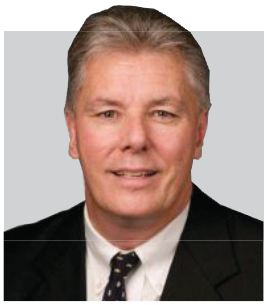
IT Intelligence

OPTIMIZE AN EXISTING SECURITY SYSTEM FOR MASS NOTIFICATION

by Bob Stockwell

Bob Stockwell is Global Technology Leader for STANLEY Security. From 1997-2012, he was Niscayah's Director of Systems Operations.

bob.stockwell@sbdinc.com



With an increased awareness of domestic threats — whether it is an active shooter situation, biological threat or other event — many companies are looking to establish effective ways to notify those people that are directly and indirectly affected. There are several valuable solutions for notifying a population of an emergency or event, but before your client invests capital to purchase the latest solution, as the security integrator you need to help companies examine the features for mass event communication already available.

Most enterprise security applications have notification functionality built in, or can be upgraded to support basic messaging requirements. Encourage your end-user organizations and institutions to take advantage of these systems, understanding that any event detected by an access or video surveillance control system can be used to trigger a notification.

Consider merging other systems with the enterprise security platform you've installed. For example, any environmental, lighting or telecom applications can be integrated into the system and programmed to trigger an alert. These events can be as simple as sending an E-mail or SMS text to a supervisor, or as complex as notifying distribution groups based on the type and severity of the event or threat. Even if the system is not set up to send SMS messages, all major mobile providers can convert an E-mail to an SMS. For instance, sending an E-mail to a specific phone number at the carrier's domain (ex.: 555-555-5555@txt.att.net) will deliver the message via text to a phone that is not set up to receive E-mail.

If a client's location also serves as storage for hazardous or restricted material, security integrators can explain that they might consider tying their detector systems to the alert. A bio or chemical detector can trigger an alert to communicate evacuation procedures, or signal individuals to stay in place and avoid a threat or accident.

Most visitor management systems can also be tied into local and federal databases for identifying known felons and offenders. Even those systems that are not integrated with external databases can build their own watch lists, and all can be used to trigger notifications.

Existing video systems can also be crucial in delivering event notification. Even an event as simple as detecting intrusion or motion in an area that should be closed off or empty can be used to warn populations of a potential threat.

Customers can also take advantage of today's advances in analytics, which can detect events that previously required human interaction. For example, there are analytics for detecting objects left behind or ones that have been removed. Analytics can perform functions such as object counting, detect loitering, detect crowds where there shouldn't be or recognize graffiti and vandalism. Facial recognition programs are improving every day and can be used to detect both approved and unapproved individuals.

After assessing the functionalities already in place through the existing enterprise security platform, integrators can work with clients to research ways to expand the alert system and notification capabilities. There are many choices, such as desktop pop-ups, virtual panic buttons or a phone dialer that plays a recorded message detailing an event or present threat. Digital signage can augment a system and offer detailed instructions or event information. Some systems include hardened modules that are PoE or wireless capable and can be placed in hard-to-reach areas. Others incorporate local, regional and national databases to display threats and make populations aware of issues in surrounding areas. Some systems have the ability to track individuals by GPS and alert them based on their locations.

Most enterprise security applications have notification functionality built in, or can be upgraded to support basic messaging requirements. Take advantage of these systems.

In communicating the details of a threat or event, the end-user client's target audience should always be considered. While many people are comfortable with phone, text and E-mail, it might be quick and effective to reach younger audiences additionally through social media. Twitter has proven time and again that it can disperse information as fast as any source of communication.

The options for communicating alerts and notices both internally and externally are expanding daily. But by analyzing the functionalities of the existing security platform, security integrators may find ideal communication methods or media options for their customers already exist within the security enterprise itself. SSI