Social Media Meets Enterprise Security

WITH THE EVER-EXPANDING AVENUES of social media, people have become incredibly dependent on the ability to share and consume content in real-time, as events unfold in both their business and daily lives. The challenge and opportunity created by these social media channels is to carefully harness the immediacy of the medium with the power of enterprise security, creating a safer environment across a broad range of vertical markets, including health care, government, energy, higher education, K-12 and other large campus settings.

Without question, social media is rapidly becoming a critical tool for global security planning, data gathering and reporting, delivering timely situational information from across the globe and from a multitude of sources. Swift notification of vital information to physical security platforms can greatly reduce the likelihood of any number of catastrophes by activating and securing facilities in advance of events that may occur.

Linking Social Media With PSIM Is Key

Given the adoption of today's unfiltered social media networks — Twitter, Instagram, Snapchat, Facebook, LinkedIn, etc. — virtually anyone can freely post any form of content that has the potential to go viral, creating significant challenges for even the most secure facilities. In the security industry, these social networks are often referred to as "social data conduits." They offer unique information streams that can be integrated into the real-time framework of today's modern physical security information management (PSIM) platforms. PSIM platforms constitute a category of software that includes applications and platforms created by middleware developers, and are designed to integrate multiple disparate security applications and devices to control them through a single, comprehensive user interface. Connecting social media to the PSIM environment would be a natural evolution in providing the PSIM user with more information to help make better choices during potentially traumatic situations.

Facial recognition represents the best opportunity for advanced warning of potential threats if social media is integrated with traditional security platforms and infrastructure.

The higher education and K-12 environments are great examples of exhibiting how social media can work extremely well by instantly processing crucial information from teachers and students. For instance, in the event that an active shooter is roaming the facility, social media updates can deliver immediate notification to those on campus currently seeking shelter. Additionally, through remote access software, campus security staff working with law enforcement can react much faster to lock down areas where other victims might be sheltering, and can provide first responders with real-time video surveillance of suspects within the facility, thus helping to create a safe entry and exit path for victims to be rescued.

Social media may also be the master of "mustering information." The integration of highly analyzed and filtered social media content from mobile devices, combined with today's enterprise security platforms through command and control centers, can provide vital mustering requirements during campus emergencies. When campus security officials need to account for 40,000+ students and staff after or during an event, the task can be daunting, at the very least. By using social media, officials can process text messages or posts to confirm the location of mobile devices, and then compare the student ID credential information stored within the PSIM to confirm the exact location, thus creating a two-factor process for verification that the student or staff member has been accounted for and located.

Photo Swell May Spur Facial Recognition Progress

Social media has also begun to merge with facial recognition capabilities. Since the 9/11 terrorist attacks, security equipment manufacturers have been working to create a stable, commercially viable product that can identify and alert when a person of interest is detected within a camera's view. This progression has been an uphill battle, with camera resolution and environmental issues plaguing the development.

Now, with the widespread popularity of social media and photo sharing, many new mobile apps and filters are becoming increasingly available to the public, and offer a plethora of capabilities to scan digital photos and find like persons within the images in a high-speed format. This provides another great opportunity to create new integration with security-based PSIM platforms that record volumes of video that are often just archived and reviewed only when events dictate. Facial recognition represents the best opportunity for advanced warning of potential threats if social media is integrated with traditional security platforms and infrastructure.

As the value of social media's immediacy is realized within the security industry, partnerships are just being formed in the OEM marketplace with social media providers. The success of these partnerships will require hardware and software providers to work closely with content providers to create new platforms that will share information, by exception, to establish safer public environments and more proactive strategies in the event an emergency or incident occurs. By responsibly incorporating security measures with the real-time data posted constantly to social media, the security space can help to usher in a new era of alertness, awareness and protection. SSI

BOB STOCKWELL is Chief Technology Officer for STANLEY Security. From 1997-2012, he was Niscayah's Director of Systems Operations. He can be reached at bob.stockwell@sbdinc.com