edCircuit
Powering the Global Education Conversation

DECISION MAKERS   **EDUCATORS**   **BUSINESS**   **INNOVATION**

BUSINESS

School security beyond walls: A Q&A with Mike Richez

BY ADMIN • MAY 11, 2015

EdCircuit recently had a chance to talk with Mike Richez about school security and approaches that schools and businesses are taking to address this issue. Richez is the Executive Vice President of Business Development for OSC World and a former school administrator. He offers his insights to us in this Q&A.

EdCircuit: In general, how are school officials responding to security threats that occur in social media? What are some of their options?

Mike Richez: In most cases, school officials have to use law enforcement, who have to follow up relative to these security threats. This takes precious time away from addressing real-time access by school officials or their in-house security staff, and being able to be proactive rather than reactive in preventing a real threat. Most threats are publicly communicated by the threatening individual, either through Twitter or Instagram and can be available with the appropriate tools.

Q: What is your company, and what is its response to handling these threats?

A: OSC World is the sole distributor of Digital Fly, a cloud-based application which monitors Twitter for potential threats. This application provides administrators and law enforcement/security personnel the ability to access public messages from these social media outlets in real-time, thereby providing alerts before a threatening individual can follow through on a real threat.   Instagram will be added during the Summer, and Facebook in the Fall. Other social media platforms will continue to be added as they crop up.

Q: How does a system like this work? What types of social media are covered?

A: Digital Fly creates a geofence around a school district or community using latitude-longitude coordinates. Filtered words and acronyms are added to only provide searches that pertain to threats, bullying, fights, gangs, etc.

Q: How has it been received so far?

A: OSC World has had hundreds of inquiries across the country since its rollout in January, 2015.

Q: How does law enforcement work with this?

A: Law enforcement would have a greater sphere over their geofence, to incorporate a greater area, and would be able to create watchlists for certain individuals who continually present a threatening nature.

Q: What about the privacy issue? How would you respond to those who say they see a conflict with student privacy?

A: Digital Fly only searches and monitors public messages. Any private or peer-to-peer communication is not available and will not be compromised. We are only reporting what individuals are communicating publicly.

Q: What about monitoring peer-to-peer social media? Is that something that can be done?

A: Peer-to-peer social media represents private communication, and can only be accessed by law enforcement. We therefore will not be including Snapchat or Yik Yak at this time.

Q: In your experience as a district administrator, you had to evaluate a lot of technology. What advice would you have for administrators who are trying to determine the best security applications for their districts?

A: Administrators should be aware that there are many security applications and that they fall under these categories:

Security Cameras with recording capabilities, playback and retention time – High definition digital rather than analog cameras are recommended with servers specifically designed for HD retention and playback. This allows for very clear images and playback whether during the day or at night.

Access Control Systems – Preferably, keyless, ID card entry for staff, with a direct relationship to installed High Definition security cameras. Minimize the number of exterior doors that allow staff and students entry and allocate one (1) entry point for visitors.

Visitor Management – At a designated door entry for visitors, a computer software management system which reads an individual's driver's license, and produces a pass that allows entry into a building for only specific meeting with the designated staff.

Social Media monitoring – Real time access to public messaging (i.e., Twitter, Instagram) to monitor potential threats to staff and students (i.e., bullying, fights, gangs, weapons, drugs, self-harm).

Security personnel, law enforcement, or designated staff to address all of the above.

Q: How does a social media monitoring system differ from the video surveillance we've become accustomed to?

A: Video surveillance provides forensic information, whereby security can view an issue which has already occurred, unless a security team is actively watching monitors, and in that case there is no pre-existing alert to prevent what is actively occurring. Social media monitoring provides a proactive approach, alerting the potential of a volatile situation prior to it actually occurring, and thereby having the ability to address and prevent.

Q: What's the role of parents and the community in helping to promote a safe school environment?

A: Now that even elementary students have cell phones, parents need to be vigilant in ensuring they are involved in monitoring their children's communications. Additionally, PTAs must be involved with their Boards of Education and Superintendents in working together to develop a safe-school initiative. This will allow for all of the stakeholders to become a cohesive unit and ensure a safer environment. Open communication among parents, community leaders, school administrators and teachers can only lead to a more positive culture.