An integrated approach

A solutions focus is always going to be more effective than buying and installing security systems piecemeal

By Karen Evans

Security systems in a typical enterprise environment often include video surveillance cameras, access control, alarms, ID badges, entrance and exit gates, security officers, and more.

Depending upon business needs and budget, an enterprise might add a mass notification system, duress buttons, intrusion sensors, biometrics and analytics. On the horizon are drones, artificial intelligence, robots, and more. That’s a lot of security and system technologies to manage!

That’s often how enterprise security is purchased and installed — as disparate pieces of equipment and systems, each serving its own specific purpose.

Yet, that also means that enterprise security solutions can be challenging to research, evaluate and purchase. Adding to the dilemma is the major consideration of initial purchase price, operating cost and system management, in addition to finding a solution that is scalable to accommodate a facility’s future needs.

There is no single solution that will provide the comprehensive security coverage that’s needed to mitigate all security risks. By implementing security technology as individual tools, and not integrated solutions, many facility security managers are missing out on the opportunity to provide even more control, convenience, cost savings, and efficiency to their organization. In reality, all components should be viewed and function as one integrated layered security system, especially for emergency management.

Each layered solution will vary from one facility and location to the next based upon a security management’s specific requirements such as size and location(s), number of employees and visitors, and other factors such as the type of business and services that it provides and the level of desired security. However, there are foundational elements that should always be included when configuring a layered security system, such as securing the perimeter, access control, emergency communications, lockdown capability, and video surveillance.

Perimeter Security

Secured entrances and exits, no matter their location, are necessary to track the many visitors, employees and contractors that can enter and exit a building each day. In many cases, door locks are connected to a centralized access control system that is monitored by security personnel and can be quickly opened during an emergency or incident. Entry control points can be easily established to only allow authorized individuals initial access to a facility or to specific areas within it, while also restricting access to high-profile areas. Additional safeguards to control entry points may include the integration of turnstiles or security doors, mantraps, video surveillance with analytics, visitor...
Video Surveillance
A video surveillance system is a useful security tool for any facility, big or small. The use of video surveillance can resolve many security incidents that arise and help document liability issues. Organizations that choose to install IP-based video surveillance systems can take advantage of the benefits of digital storage, remote monitoring, and analytics capabilities that may deter crimes or security incidents.

Emergency Communications and Lockdowns
According to a 2016 estimate from the Office Of The Parliamentary Budget Officer (PBO), in the fiscal year 2012-2013, the Disaster Financial Assistance Arrangements (DFAA) program transferred $280 million to the provinces. By 2013-2014, this had increased to $1.02 billion and $305 million in 2014-2015. DFAA estimates its transfers resulting from previous events will be higher in subsequent years ($848 million in 2015-2016, $590 million in 2016-2017, and $580 million in 2017-2018). The unpredictability of any severe weather event can force a facility to temporarily lockdown and restrict access. In these types of situations, system-wide communication is a critical asset to help security staff and first responders evaluate a situation and determine the most appropriate course of action. Accurate information provided via internal communications delivers real-time situational awareness that enhances overall physical security.

An Integrated Solution
When combined, perimeter management, access control, video surveillance and emergency communications are the foundation for a safer facility. This foundation can be vastly enhanced when integrated into a single emergency notification platform, which provides an effective resource to issue alerts and manage a variety of situations such as inclement weather, natural disasters, workplace violence, and more.
These specially engineered emergency notification solutions provide vital emergency status details to first responders so they can best help enterprise security manage events. A security team can issue an alert to notify responders of conditions in real time while communicating details based on the level of the alert. Employees and staff can report their specific location, enabling first responders to view detailed facility maps with room-by-room, colour-coded conditions that are updated in real time as the situation evolves. Staff members who are logged in can use a chat feature to enable two-way communications, issue messages with response instructions specific to each alert level via email or text and override any computer on a facility’s network to ensure the highest visibility of alert status.
A solution that is browser-based can function across LAN, Wi-Fi, WAN, or high-speed cellular service to offer maximum accessibility. Audit trails can be provided with chronological event sequences that can capture who/what/when/where an incident occurred, providing security staff with valuable forensic details for investigation purposes. Perhaps one of the most comprehensive safeguards of an emergency notification solution is the ability for a facility’s security team to create a lockdown alert level and push that notification out to employees in seconds while simultaneously locking all doors and blocking credential readers to everyone except authorized responders.
Security management faces tremendous pressure to protect the people and assets they oversee, especially in the case of an emergency. And most often they are supposed to do so with tight security budgets. That's even more reason to remove the security component mentality and purchasing practices and instead implement a complete and layered security solution. Simply put, layered security solutions offer superior protection and risk mitigation. When tough choices need to be made, a layered management system provides a “better” solution while being cost-effective, powerful and scalable. It's the key to making an enterprise safer and more secure.

Karen Evans is the CEO of Sielox LLC (www.sielox.com)