Photos courtesy of the Electronic Security Association

Improvements in Electronic Security at Schools

Begin at the Entrance

By Marshall Marinace

THERE HAVE BEEN DRAMATIC ADVANCES in electronic entrance and egress security in recent years, and in no industry has this been more visible and necessary than in the world of education.

With recent tragic events at every academic level, schools and universities are seeking out the most effective and reliable electronic security systems for either partial upgrades or completely new installations. Manufacturers are responding with solutions that dramatically improve access control, intrusion detection, security monitoring, building networking and communications with law enforcement.

Solutions Made for the Right Grade

There are two distinct markets within education when it comes to electronic security installations: grades K-12, with teachers and administrators controlling most of the access, and higher education, in which students themselves may have access control devices such as key cards, fobs or badges.

Perhaps the most common access control application seen today in the elementary through high school grades is pre-scheduled locking and unlocking. In these schools, administrators set a time period at the beginning of the school day when a school's main entrances remain unlocked—for example, between 8:00 and 8:30 a.m. During that time, a school official stands inside the doors and checks students in as they enter the building. Then, at the end of the period, the main entrance doors automatically lock. After that time, guests need to ring a video intercom in order to be buzzed into the building.

In K-12, only administrators and faculty carry access control cards, fobs or badges. The primary reason is that younger children simply are more prone to losing these types of devices. What's more, there is far less of a need for key cards and fobs in smaller schools with fewer buildings and entrances.

On the other hand, access control in higher education is more sophisticated, with students being issued electronic access control cards (which they can carry in a wallet or purse) or fobs (which attach to a keychain). Key cards are probably the most popular device, as they can also serve as photo IDs and are relatively inexpensive to produce and purchase.

Pin codes entered through a keypad are a much lower form of security that are used by some colleges on interior doors leading to lower-security areas such as lunchrooms and offices.

Also, in higher education facilities, multiple buildings can be networked through a main control station with a central database. This database not only controls locking and unlocking of key entrances and exits but can also house information attained from key cards. Administrators can monitor who has gained entrance to a locked room, such as a science lab, and exactly when they entered and when they left.

Controlling Any Situation

In any educational environment, administrators are now able to control entrance and egress access from a central station. They may even be able to use a PC, tablet or smartphone for access control from an off-campus location. This level of control can be crucial when a situation requires a lockdown.

Today it is essential that facility managers, administrators, teachers and area law enforcement all have the ability to immediately implement a lockdown.

The most common form of lockdown is implemented from directly inside the building. Today it is essential that facility managers, administrators, teachers and area law enforcement all have the ability to immediately implement a lockdown. Some schools are issuing wireless remote buttons to school staff that can be worn around their neck or attached to a belt. When the button is pushed, all entry and classroom doors are locked, and an intercom message announces that a lockdown is in place, with the appropriate instructions delivered to students and teachers.

When conducting an overall security assessment and setting up lockdown initiatives, the goal is to keep intruders out of the building. For safety reasons, it is also essential to ensure that people in the building have free egress. Doors locked from the outside must allow exit, whether through using a key card, panic bar, request-to-exit motion detectors or a simple door release button.

Meeting Demand—and Safety Codes

Today the demand for the most effective electronic security systems in schools is higher than ever from parents and communities that are all too aware of the dangers of allowing entrance to the wrong person. Fortunately, there are fewer barriers to schools that want to implement these systems. Of course, funding for schools is always tight and has to be approved, but many local governing bodies recognize the importance of school security. Additionally, the cost of access control systems is going down, the result of mass-production of equipment and the increased availability of these systems.

Installation time is also shorter than ever before. Architects and engineers are designing doors that are fortified with thicker metal, extra-strength

hinges and bullet-proof glass. Some doors even have electronic locks pre-installed by the manufacturer.

In addition to meeting public demand, schools also have to meet safety codes. Organizations like Underwriters Laboratories (UL), Intertek, the International Code Council (ICC) and the National Fire Protection Association (NFPA) regularly establish and update codes and standards for the installation of electronic access control in a range of industries, including education. It is up to individual states to adopt some or all of these codes, which vary from state to state as a result. Therefore, it is essential for school administrators to keep abreast of the latest ordinances that govern their buildings in order to maintain the highest level of security.

The Electronic Security Association® (ESA) maintains a Codes and Standards Committee that is constantly reviewing these guidelines and working on ways to update and improve them. ESA has developed electronic school security guidelines that are designed to assist school administrators as they reevaluate their security plan. The guidelines are available to everyone (including non-members) on the EAS website (www.ESAweb.org/schoolsecurity).

ESA is also working on a large undertaking with the Security Industry Association (SIA), a coalition of representatives from law enforcement, architects, engineers and designers. The project will produce a series of policy papers and white papers, all evaluating the security needs and proposing appropriate solutions for schools.

Setting Solutions in Motion

Although most funding for school security currently comes at the local level from states and municipalities, ESA has a Government Relations Committee that is focused on support for school security allocations at the federal level. This committee works closely with ESA's Director of Government Relations, John Chwat, who is well-connected on Capitol Hill and who works diligently to set up meetings with members of the House and Senate, as well as with organizations like the National Schoolboard Association, the National PTA and the National Association of School Superintendents.

By educating these organizations and federal bodies on the latest security technologies, ESA is working toward the ultimate goal of increasing fund allocations to schools and districts through federal grant programs. It is trying to ensure that federal funding goes beyond dollars allotted for counseling, mentoring and research to include the purchase of effective electronic solutions that meet and even surpass codes and standards—electronic security solutions that can save lives.

About the Author: Marshall Marinace is President of the Electronic Security Association (ESA). He is also owner of Yorktown Heights, N.Y.-based Marshall Alarm Systems. In his 38 years in the security industry, Marinace has served in many capacities as an ESA volunteer. He is also a past-president of the New York State Electronic Security Association and the Westchester, N.Y. Alarm Association.