Article

Securing the weakest link

In 1999, just 19 percent of public schools reported using security cameras.[1] By 2013, that number had increased to 75 percent.[2] It is estimated that by 2018, schools will spend over $1.1 billion annually on security infrastructure,[3] but the majority of these funds are being invested in video surveillance systems,[4] which are used almost exclusively to analyze events after they have occurred, rather than preventing them happening in the first place.

The balance of available security funds is being focused on the most visible points of entry such as the front entrance, while secondary access points often remain vulnerable to unauthorized access. Because the traffic through these openings is much lower, it is estimated that only half are equipped with an electronic access control system.[5] Not surprisingly, over 55 percent of schools surveyed reported that their secondary doors were frequently left unlocked or propped open, with 22 percent stating that this occurs on a weekly or even daily basis.[6]

As a matter of convenience, latches are taped, pebbles are placed in strikes and door stops are used to prop open these doors. The most common culprits are the students and teachers who occupy the building, but neither the students nor their teachers are likely to have received any training on the inherent security risks of such behavior. The resulting unsecured access point creates vulnerabilities that not only compromise the building's everyday security, but could also limit the ability of administrators to effectively lockdown the facility in response to an emergency event.

Securing the perimeter

One of the most important steps in securing the perimeter of a facility is to control the flow of people entering and leaving. Many schools rely on security checkpoints to prevent weapons and other contraband from entering the school, but these are easily bypassed if students can gain access through unsecured secondary entrances. After years of steep budget cuts, most schools lack the necessary funds to purchase and install traditional access control systems on their secondary openings. As a result, physically touring the building to dog and undog doors and check security status is still the predominant of managing these openings.

> "Doors that are unlocked or dogged and unmonitored provide means for intruders to enter the building. The time is takes to manually unlock doors for arrival, and then lock them after arrival, is significant."
>
> – **Paul Timm**, PSP, a board-certified Physical Security Professional with Facility Engineering Associates.

Timm is the author of *School Security: How to Build and Strengthen a School Safety Program*, and a nationally acclaimed expert in school security. He notes that relying exclusively on physically touring doors also means that any time an emergency situation warrants a lockdown of the school, janitorial staff must manually lock all of their secondary openings – a procedure which could take a significant amount of time to complete and potentially put school staff into harm's way.

Controlling access is key

"Access control is the cornerstone of effective school security," says Timm. "Schools cannot furnish a safe learning environment without controlling and restricting access and being able to account for students and staff."

In searching for a solution to the problem of lax perimeter security, school officials often become overwhelmed or discouraged by the projected costs of installing additional access control hardware on secondary openings.

The first step to addressing the problem is to designate a single, primary point of entry for school hours. This is preferably a front door location that is easily seen and supervised to provide more control over who should – and shouldn't – enter the building. The main entrance should be clearly marked by signage with directions to a secure

[1] NCES
[2] NCES
[3] TechNavio
[4] TechNavio
[5] Ducker
[6] SMARI

vestibule that will serve as the visitor management center. Creating one primary location for individuals to enter the building creates a far more secure environment and decreases the risk of students carrying weapons into the facility undetected.

Of course, the only way to ensure that all students, faculty and visitors use this primary point of entry is to ensure that all other points of entry are secure at all times. Ideally, all doors will be closed and secured, creating a closed campus environment where access is strictly monitored and restricted. However, if this is not feasible for the campus then the goal should be to at least reduce the number of exterior openings to as few as possible.

An effective way to achieve this is to establish guidelines for the use of each opening. You will need to outline the following details for each door on campus:

- When will the door be locked and unlocked?
- How will it be staffed or monitored?
- How will it be secured?
- How will security be enforced?
- Who is and is not allowed access?
- How will authorized users be granted access?

Unsecured and unmonitored doors have the potential to allow two types of events to occur unnoticed — either an uninvited guest entering or a student exiting. Often times, an entry point becomes compromised when a teacher or student props it open. There are a number of security devices available to ensure that all points of entry are secure at all times while still allowing free egress in the event of an emergency.

Extending access control

In order to effectively secure a campus, all secondary entrances should be incorporated into the access control system, either directly or through the installation of electro-mechanical locks that are connected wirelessly to the existing system.

Mechanical and electronic technologies continue to converge, leading to the creation of wireless electro-mechanical hardware that is significantly less expensive and easier to install than traditional wired solutions.

When evaluating the available options, look for solutions that are proactive rather than reactive. Obtaining a recording of a crime via video surveillance is not nearly as effective as preventing the situation in the first place by ensuring the campus is completely secure.

Another feature to look for is open platform hardware that will be allow the system to be compatible with any existing or future software. Interoperability is a major factor in terms of security, operational efficiency, and convenience. Access control solutions that do not work well together will cause challenges for administrators and users. Whether the impact is the need to issue multiple credentials or manage multiple access control software platforms, lack of interoperability drives inefficiencies that put more strain on limited resources and create inconvenience that can ultimately lead to compromises in security.

Consult the experts

While these steps are an important part of enhancing perimeter security, school officials should hire a professional integrator to develop a scalable, long-range, comprehensive security plan for their facility. These security experts can play a vital role in helping to identify and prioritize the security measures that need to be implemented.

> “An effective physical security assessment will identify both strengths and weaknesses of your security program. More than simply identifying vulnerabilities, a good assessment report will prioritize recommendations in a phased approach.”
>
> – Paul Timm

With the number of available security products, the selection process can be overwhelming. Security integrators can ensure that the system or products installed are successful, appropriate, code-compliant and cost effective.

Given the potential ramification of the decisions that have to be made, the importance of choosing a quality, professional security integrator cannot be overstated. Insist on professional references and be thorough when interviewing to determine if they will be an effective partner for your project. While controlling costs in an issue on any project, particularly in light of the budget cuts many schools have had to contend with, this is not the area to cut corners.

Hiring a quality integrator will prevent unnecessary expenses, ineffective or incompatible products, and the potential liability that could result from code violations. For example, there are a number of security products such as barricade devices that are being marketed to schools as an inexpensive and effective means of enhancing classroom security. However, the majority of these products violate model building codes and actually create additional threats to life safety. Professional security integrators will be aware of these potential code violations and can help ensure school administrators focus on safe, reliable and cost effective solutions.

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage®, SimonsVoss® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

KRYPTONITE ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION™