HAGER COMPANIES
Published in the Doors + Hardware Magazine, June 2017

Solution Trends in Educational Facilities

by Brian Clarke, AHC, CDT, CSI

Violence in schools; it seems we hear about it daily.

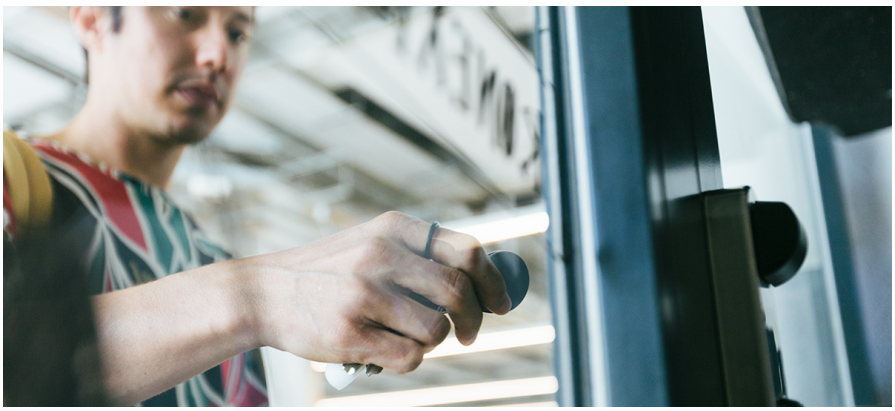
A 2015 fact sheet on Understanding School Violence, representing a sample of youth in the U.S. from grades 9-12 compiled the following statistics:

- 7.8% reported being in a physical fight on school property in the 12 months before the survey.
- 5.6% reported that they did not go to school on one or more days in the 30 days before the survey because they felt unsafe at school or on their way to or from school.
- 4.1% reported carrying a weapon (gun, knife or club) on school property on one or more days in the 30 days before the survey.
- 6.0% reported being threatened or injured with a weapon on school property one or more times in the 12 months before the survey.
- 20.2% reported being bullied on school property and 15.5% reported being bullied electronically during the 12 months before the survey.

While in the process of writing this article I received a news alert on my smart phone that one person had been killed and two injured in a stabbing at the University of Texas at Austin. There are and have been many ongoing discussions on the best way to prevent these horrible occurrences. The door and hardware industry have been focusing on the two things they know best: doors and hardware.

In the aftermath of the Columbine tragedy in 1999 the classroom intruder function was developed allowing a lock to be secured from the interior of a classroom, while still allowing free egress from the inside and entry from the outside using a key. Technology has continued to improve since that time and today there are many options to securing a classroom and other door openings, including mechanical, electro-mechanical and, most recently, electronic.

Many offline electronic systems use a portable programming device to transfer audit data from the locks to the software as well as to update the locks with the user credentials and calendar information.



These type of systems obviously require the administrator or maintenance department to visit the individual locks to make any changes which can be cumbersome and time consuming. In those cases, the lock is the component which makes the decision to allow or disallow a given credential. Some offline systems can be easily upgraded to become part of a virtual network or a wireless system, which gives start-up users or small schools the flexibility to grow and improve their systems as their needs change.

Data-on-Card systems provide flexible security by using a credential to transmit system data between offline devices and online management systems. All user-related access information is stored on smart credentials that act as carriers for the network. This eliminates the need to have wired or wireless locks at every secured opening and drastically reduces the overall cost of the access control system. In these cases, it is the card that has the access rights and signals the offline lock how it should respond.

Wireless and hard-wired systems can be used when immediate checking on the opening are needed. They are designed to offer real-time monitoring and control, including in many cases lock-down abilities, and are highly recommended for institutional, educational and commercial applications requiring enhanced levels of security.

With all these code-compliant, free egress security options offered in the marketplace and the cost of systems reducing at every turn, you would think that more users would have embraced the available options.

Unfortunately, there has been a rise in the recommendation of so called “barricade devices.” These products, while securing a door opening from unwanted ingress, do not take into account the fire or building codes that have been put into place to maintain safety for occupants and first responders. A few states have passed laws that allow these devices to be used as viable options, against the advice of their state fire marshals, building code officials and various other officials.

A report by Ohio’s building codes board, which was critical of the devices, stated the devices are “unlisted, unlabeled and untested.” Lawmakers in Ohio approved the devices following testimony from manufacturers of the devices and parents of school children. Several Door and Hardware industry experts also testified against the use of such products but to no avail.

“There are many factors in determining which type of door hardware and access control applications work for a facility therefore conversations between the architect, end user, specification writer and general contractor are imperative,” says Sheryl Simon, Senior Architectural Specification Consultant with Hager Companies.

However, there are other parts of the equation which are often forgotten in the design of a security system. The user experience is one such part, while mobile integration is another.

Users are the most important part of a security strategy, yet often times the weakest link, putting themselves and others at risk when they don’t do their part. Propping doors open and granting someone access who forgot their card are just two examples of users not doing their part in keeping their environment secure.

Like any technology, access control has evolved over the years. As a result, solutions now offer more security and convenience than ever before. Advancements in “intelligent” products are making it easier, and to some extent even appealing for users to comply with requirements. By implementing an access control solution that is attractive to its users, institutions can significantly reduce user error risk factors. While it might seem like common sense, it is important to remember that the more attractive or “cool” a solution is, the greater chance users will comply.

Part of creating a more user-friendly experience is the introduction of a single, comprehensive credential that can be used to gain access into a building but also contains enough data compartments to integrate with other systems. Being able to eliminate unnecessary steps makes it easier for individuals to use the system that is in place to protect them. Many schools and universities are starting to combine ID cards, library cards, meal plans and dorm keys into one single credential thus providing students, faculty and staff a much more user-friendly experience.

Highlighted by the growing demand for universal broadband access, mobile integration is one of the largest growing areas within the access control industry. As consumers continue to integrate their phones more and more into their daily routine, there is an opportunity for the security industry to capitalize on society’s dependency for their hand-held devices.

In the past several years, phones have developed into a method of identification, payment and banking. Using smartphones for access control allows for a more seamless experience, as well as an efficient way to merge security and convenience. While mobile-centered access control might not be ideal for primary schools, it does provide a unique opportunity for schools, colleges and universities.

With a cell phone in almost every student’s hand, it makes sense that technology and applications are popping up to help students not only get around campus, but more importantly, make sure they stay safe doing it. Implementing a more mobile-friendly access control system in educational institutions will provide schools with the access control and security they need while also providing students with a more user-friendly and convenient experience.

Clearly, the access control world has been simplified considerably as technology has advanced. Those companies who tended to avoid electronics as being “too difficult to set up” and “not user-friendly” will be pleased to see this trend emerge as it now allows them to enter the arena without so much trepidation. Also, it gives contract hardware distributors an important complementary revenue stream. As they strive to offer more and more “all inclusive” packages to the owners and end users, this is an opportunity not to be missed.

BRIAN CLARKE, AHC, CDT, CSI, is Director of Architectural Specifications and Technical Support for Hager Companies. He can be reached at bclarke@hagerco.com.

HAGER COMPANIES