SORENSEN & WILDER Associates

Specialists in Safety and Security Solutions

CREATING AND MAINTAINING A SECURE SCHOOL

By Steven S. Wilder

Is a secure school an attainable goal, or a mythological fantasy? In lieu of recent incidents of school violence, more and more school administrators are expressing doubt that a school can truly become a secure environment. Fortunately, a secure school is an attainable goal if a systematic approach is taken.

Too often, school administrators turn to cameras and metal detectors, thinking that these are the critical elements of a school security program. What they often fail to realize is that technology is but one of four critical components that must be considered for a school security program to be complete. Referred to as the P2T2® system, an effective security system must contain the right complement of four basic elements: People, Programs, Training, and Technology. In this article we will look at the first two elements: People and Programs. In the May issue we will focus on technology that can be used to help secure a school, and in the September issue we will address security related training for school staff.

PEOPLE AND PROGRAMS

When considering People as a component in a school security program, the focus is on making sure that only the right people are in our buildings. The emphasis on People includes certified and licensed staff, support service workers, visitors, contractors, and vendors. What do we know about the people in our building? Do we do background checks on all of our employees? Do we verify the identity of visitors in the building? Do we allow visitors to roam the hallways, or do we require that they be escorted and supervised at all times they are in the building? Do we verify the legitimacy of a visitor's presence? Do we take steps to safeguard our faculty against the aggressive acts of visitors, such as during parent teacher conferences and sporting events? What do we know about contractors and vendors?

School administrators have a fiduciary obligation to assure that proper steps are taken to prevent unauthorized personnel from entering the school and to assure that only qualified staff is put to work in the school. The People component also takes into consideration issues such as selection criteria for hiring, drug screening for employees, effective use of school resource officers and security

officers, as well as the use of exit interviews with staff leaving the schools employment.

The second component, Programs, focuses on developing and implementing a written security program for a school. While most schools have developed excellent crisis intervention programs, the majority of these programs are written from a reactive approach, and seldom take a proactive approach when addressing school security issues. A written security management plan should be developed for each school that includes quantifiable goals and objectives for the school security program, assignment of responsibilities for school security, processes in the management of school security, typical or usual security issues, incident reporting, staff, visitor and student identification programs, recognition and identification of security sensitive areas of the school, orientation and education of employees, and a statement of authority for administering the security program.

In addition to a written security management plan, individual security policies should be addressed as well. These should include staff and student parking, access and egress from the building, issuance and returning of keys, school violence prevention, discipline, security training, and others that might be applicable. In many cases, similar policies often exist, and are found buried in a different policy manual. An organized security plan brings all security related policies together under one cover so that policies and procedures related to school security can be immediately accessed as needed.

Comprehensive security assessments are another part of the Program component of a school security system. A comprehensive security assessment, conducted by a qualified security professional should be considered periodically by every school board. All too often, school boards and school administrators want to simply distribute checklists to the staff, thinking that a qualified assessment will result. Unfortunately, experience has proven that this is not a safe approach, and can often end with disastrous results. Even with the best of checklists, many school staff do not understand the workings of an integrated technology system, legal aspects of school security, lighting issues, good vs. bad training, or any of the other critical aspects that a qualified security professional would address.

Finally, post incident response must be included as part of the school security program. No school is immune to the risk of an incident, and while managing the

incident is so critical, recovery is equally crucial. A program that focuses on post incident response must be developed to provide direction and guidance during emotionally challenged times so that the needs of the students, faculty and staff, parents, and the community can be addressed and managed.

SECURITY TECHNOLOGY

Too often, we see school administrators believing that technology is the "end-all" for creating a secure school. Unfortunately, that just isn't true, as we have previously established. At the same time, technology, when properly designed and installed, is very critical to a school security program.

In simple terms, modern technology is used as a tool to assist in our efforts to create and maintain a secure environment. Typically, we look at technological systems in six categories:

a. Access control
b. CCTV and recording
c. Alarm and duress systems
d. Communication systems
e. Visitor control systems
f. Identification systems

The most commonly found systems are access control and CCTV. Unfortunately, we seldom see these systems properly designed and integrated, and as a result, they are rarely used to their true potential.

Access control systems are used to do exactly what the name implies: allow authorized access and prohibit unauthorized access. Unfortunately, many schools will spend thousands of dollars to install an access control system on the main entrance doors, while at the same time ignoring other perimeter doors, which inevitably are found propped open for staff convenience. And, if we can look at them and realize they are propped open…so can the bad guys! These types of human errors tell us a variety of things about a school's security program:

1. Security policies are likely very poorly written

2. Security policies are not enforced; staff know there is no accountability for compliance
3. The access control system was designed by a person who lacked the necessary qualifications and understandings of school security
4. The access control system is outdated, and lacks the hold open sensors that are common on today's systems

Closed circuit television (CCTV) is another area that schools often fail to use effectively. In many schools, antiquated black and white cameras tied into an aged video cassette recorder are still the system in place. The recent decline in the cost of CCTV and digital video recording systems makes it almost shameful for schools not to have the proper technology in place. Additionally, modern CCTV cameras and digital recording systems are capable of performing at levels previously unheard of, including facial recognition capability and other intelligent video analytics. The value of a modern CCTV system is found in two areas: the right system designed by a qualified designer.

Another critical concern in school security management is lobby management and visitor control. While the intent is never to embarrass anyone, when performing a school security assessment, I always enjoy the opportunity to ask the Principal or Superintendent for an immediate, up to the minute list of all visitors in the school, what their purpose is, and where they are authorized to be. Occasionally I am given some form of a "visitor log" that someone has signed in on, with what we assume is a real name. Where they are in the building or what they are doing is often unknown. And barriers meant to contain visitors or to limit access are often imaginary, or are attempted through some feeble effort such as wall signs. Again, these antiquated methodologies represent a failure to maintain industry best practices, and may even be considered a serious deviation from an industry standard. Today, modern technology allows schools to not only identify visitors, but to scan the visitor's driver's license against a national sex offender registry and determine if the visitor should be allowed in the school. With all but a handful of states having adopted some form of "Jessica's Law", a simple sign-in log is not adequate to keep child predators from entering our schools. Again, school administrators have the fiduciary obligation we previously discussed, and must exercise all reasonable measures to assure a secure environment.

Funding for new technology is always an issue, and is certainly an understandable concern. At the same time, changes in our society force schools to address the issue, and to take a realistic approach towards finding the funds.

In many states, use of life safety funds that were previously restricted to fire prevention and suppression systems are now being allowed for the acquisition, installation, and ongoing maintenance of security systems as well. And, administrators can save additional money by using a qualified security professional to determine the type system to be used, and to develop the system specifications and design engineering.

TRAINING

Training is the fourth critical element in the P2T2® system. Training is the school's opportunity to provide the knowledge to the staff to maintain a secure environment. The term staff includes uniform security staff, non-security staff such as administrators, faculty, and support service employees, school resource officers (SRO's) or law enforcement officials regularly present on site at the school, as well as information provided to families.

Training on school security be developed to the level that a school employee plays in the school security program. For example, school security officers, SRO's, and those involved with the day-to-day management of aggressive or violent students should be trained in verbal de-escalation skills, talk down techniques, as well as take down and physical restraint techniques. Conversely, those who do not play a role at that level need not receive such detailed training. At the same time, every employee in the school should be trained in basic security rules, regulations, and compliance requirements. This may include parking requirements, entering and exiting the building through various points of entry, requirement for ID badges, and other simple yet critical security related issues.

Training also gives us the opportunity to enhance our ability to provide physical protection to the people and property within the building. Many times, we see the integrity of the security management program compromised by human error. In a majority of these cases, the people who are making the errors are not doing so with the intent of compromising security, rather, they lack the proper training to realize the vulnerabilities that their errors create. Providing security awareness training to all employees is an opportunity to increase our ability to provide the most secure environment that we are capable of.

As an example, the author recently had the opportunity to visit a school that had just spent thousands of dollars installing an access control system on all

perimeter doors. While walking the school, we had the opportunity to observe the Superintendent of the district escorting a local new reporter around the building, showing off the improvements that they had made with security technology. While walking and visiting with the reporter, the Superintendent was observed opening a perimeter door and propping it open with a chair. While her actions were without malice, and she certainly had no intent of compromising security, she defeated the integrity of the access control system and left the entire school vulnerable to intrusion. No doubt, with proper training (and better system design) she would never have taken such a step.

The P2T2® system is a critical component in a school Security Vulnerability Assessment (SVA). The SVA will allow a school administrator a number of benefits including:

1. Developing an understanding of all of the possible security vulnerabilities that exist in the school.
2. Identifying a realistic threat level for each school.
3. Providing critical information needed to develop a school security plan
4. Aids in decision making for allocating financial resources where they are most needed.
5. Designing and installing security systems and equipment together with programmatic improvements designed to reduce the risk level.
6. Providing a document that can be presented to local Departments of Education and other federal, state and local sources of funding. This may result in a release of funds for security improvement purposes for the school.

Hopefully, you have found this article to be of value in your efforts to improve your school security program. School security is an ongoing challenge that is not going to get any easier. Developing and maintaining a secure school environment is an attainable goal. It is accomplished through proper use of your people, well designed programs, well-educated and trained staff, and appropriately designed security technologies. If any one of these four areas is incomplete, your program remains deficient.

Steve Wilder is President and COO of Sorensen, Wilder and Associates (SWA) in Champaign, IL. SWA provides safety and security assessments and

consulting services to schools throughout the United States, and are frequent lecturers on issues of school violence and school security. Steve can be reached at 800-568-2931, or online at www.swa4safety.com