

Keeping Watch

A series of detailed security questions can help education administrators in the long term.

By Patrick V. Fiel Sr.

A generation ago, school administrators worried about students cheating on tests, stealing from one another's lockers and maybe an occasional fight. Today, educators deal with many of the same problems facing local police—drug sales, weapons possession, arson and gang violence. By preparing for these problems, education administrators can be ready to handle difficult situations and make a serious dent in crime. Education administrators should identify potential

weaknesses in their campus security, plug the gaps and help make schools a safe haven for students and teachers.

Identifying risks

Here are some questions that every school administrator should ask as part of a risk assessment:

•**Does the current security plan protect every access point?** A combination of intrusion detection, access control and video surveillance provides the strongest protection for access points. Intrusion detectors can warn of attempted break-ins. It may be appropriate to use electronic access-control systems (cards and readers) on entries dedicated to administration, faculty and staff. Video cameras also can be mounted at critical access points to provide both a real-time and documented record of who entered a building and when.

•**Does the school have a visitor-management program to help prevent unauthorized persons from gaining access?** A strong

(Are the school's security needs and fire systems tested and inspected routinely?)

visitor-management policy can help keep unwanted persons off a school campus. All visitors should be required to check in at the school office. At elementary schools, which usually are less open than high schools, the office door can remain locked with an intercom and video camera mounted outside. This will allow school officials an opportunity to check a visitor's identity before granting or denying entry.

High schools should include a visitor badging system. After signing in at the office, all visitors should receive a temporary credential to wear while on campus. If all teachers, staff, administrators and visitors wear identification badges, any adult without one will stand out and be open to challenge.

•**Does the security plan take into account community (non-school-related programs) activities on campus?** Extracurricular activities, such as community forums, Boy Scout meetings and church services, take place in late afternoons, at night or during



Valencia Community College—Osceola, Technical Science Building III, Kissimmee, Fla.; Architect: SchenkelShultz Architecture. Photo courtesy of William Garrow

weekends when few, if any, school officials are likely to be on campus. It is easy to forget that school security is not an eight-hour-a-day job, but one that requires attention 24 hours a day, seven days a week. Available technology—intrusion control, access control and video surveillance—can play a major role in helping protect a campus when school employees are gone.

•**Does the security plan take into account fringe time periods when students and staff are arriving and leaving?** The hectic activity that surrounds the start and end of each school day (and passing periods), gives students a chance for mischief and for unwanted people to sneak into the school. These are times no staff should be in the classrooms or office. Put teachers and administrators in the hallways, at the entries and on the playgrounds where they can monitor events.

Does the current security plan protect every access point?

•**Are computers, athletic equipment and student records secured properly against theft?** Technology can help protect equipment and records. Computer and science labs may benefit from an access-card reader mounted outside the door, allowing entrance only to appropriate teachers and administrators. Electronic article-surveillance tags can be attached to portable items. That way, for example, an alarm would sound if there were an attempt to remove a laptop computer from the room. Student records are best kept in a core office space without windows and only one entry.

•**Is there a video-surveillance system monitoring, recording and storing video of vulnerable areas?** Realistically, few schools have the ability to monitor cameras continuously. But there should be a policy that provides for a regular check of live and recorded video. Also, recorded video should be kept for at least 30 days.

•**Can the video-surveillance system be monitored from a remote location?** Today's digital and networked video systems allow for remote viewing of live and recorded video. This gives authorized administrators the ability to check on the school from another location. In doing so, administrators gain a powerful tool for establishing a safe and secure climate for the people and property at a school—whether during school hours or at night and on weekends.

•**Can real-time security system data (video, audio, access control) be shared with local law enforcement?** It is possible to give local law-enforcement officials the same access to information from the school security system. This can be valuable in the middle of a potentially dangerous situation on campus. The more information police have, the more effectively they can respond.

•**Are all security systems (intrusion, access control, emergency voice, video surveillance) integrated into one network?** Integrating a school's security systems makes sense. Economically, it can

increase the effectiveness of a school's total security approach. For example, an intrusion alarm can trigger the nearest camera to begin recording events leading to an alarm situation.

•**Is the security system integrated with the IT network? Is the network safe from cyber attack?** The convergence—or integration—of the security and IT networks is inevitable. Some schools still create standalone security systems with separate cabling, but many now are integrating with the district or campus IT network and creating a virtual local-area network (VLAN) that isolates the security function on the network. But as the security function becomes dependent on the network, it is vulnerable to hackers. For that reason, it is vital to work closely with the IT staff to ensure these new “information systems” are designed and configured securely.

•**Does the system monitor for hazardous fumes, such as carbon monoxide? How quickly is staff alerted when a critical system, such as the air conditioning or furnace, becomes inoperable?** It is easy to add sensors to an HVAC system that will create an alarm should a critical system fail or carbon-monoxide levels rise to dangerous levels. These alarms can be monitored at the school, district or campus, or by a third-party alarm-monitoring center.

•**Are the school's security needs and fire systems tested and inspected routinely?** The security and life-safety businesses are changing constantly, requiring regular review and updating of policies and systems. Equipment maintenance, such as cleaning smoke detectors, or camera lenses and housings, is important. It may be convenient and cost-effective to have an inspection and maintenance agreement with the institution's security equipment provider.

Other tips

A safe and secure school begins with a good security plan that can be customized for each campus. In designing that plan, it is important to solicit input from local law enforcement, community members and parents. Bringing in a safety expert also can provide the plan with a different perspective. And do not forget to include the students—they are the ones that really know what is happening in the school. Once a plan is adopted, be sure to include proper training for staff and students.

Also, do not overlook the campus' outdoor areas in the security plan. Look for and eliminate building features that provide access to the roof or upper stories, such as fences attached to the building or other elements that provide hand- or foot-holds. And, if possible, avoid landscaping that obscures observation from outside the campus and provides a place to hide weapons or drugs.

Develop a “safe corridor” program that helps students travel safely to and from school. Many students have said they fear for their safety during the commute. ■

Fiel is a public safety adviser specializing in education for ADT Security Services, Inc., Alexandria, Va. For six years, he was executive director of school security for the Washington, D.C., Public School System, where he managed 163 school campuses.