ERIC DIGEST

FEBRUARY 2001 NUMBER 145 EDO-EA-01-02

Newer Technologies for School Security

By Tod Schneider

School officials may decide to consider technological solutions to security or crime problems when less invasive measures have proved inadequate or too costly. When unwelcome intruders, including armed individuals, are the targeted problem, schools can select among several categories of technology: (1) keys and smart cards, (2) metal detectors, (3) alarm systems, and (4) surveillance equipment.

Before resorting to high-tech security solutions, school officials should think carefully about the possible (and unintended) consequences of security technologies. They may reinforce fear, undermining the social ecology of the school. They may be a mismatch for the problem being addressed. They can be expensive. And they require ongoing maintenance, repairs, and upgrades that need to be included in the budget.

This Digest describes several technologies that can be employed to control access and to improve surveillance of school grounds.

What Technologies Can Be Employed To Improve Access Control?

In many schools, lost and/or duplicated keys have led to theft or other problems with unauthorized visitors. In such cases, alternative entry-control devices should be considered.

Various types of "smart" cards have become a common means of access control. These card systems, issued to staff and vendors who require access at varying hours, are generally integrated with computer software that allows for very specific coding. For example, each card can be tailored to an individual's needs; a cook can be allowed off-hours access to the cafeteria, but not the administrative offices.

Smart cards can be instantly cancelled in case of card loss or theft, so they will not work if someone subsequently tries to use them to gain entry.

The cards may be swiped through a slot (swipe cards), or they may merely need to be held close to a reader (proximity cards). Contractors can be issued access cards coded to allow entry only for certain days or hours. Parking-lot access can be controlled, allowing students to enter and exit only before and after school. The cards can also serve as identity and debit cards.

Smart-card technology eliminates the expense of replacing or altering locks and keys. The downside is the initial expense for the electronic entry (about $500 per door), card production, computer, card-printer, and scanning equipment. These costs exceed those of conventional keys in the short run, but the security options are far better.

Are Metal Detectors a Wise Investment?

The vast majority of schools in the United States have not had school shootings, nor do they have reason to expect shootings to take place. Metal detectors are hard to justify in such low-crime settings, and may undermine a school's atmosphere. Unfortunately there are other schools where metal weapons are a serious, ongoing problem. In those settings, detectors are well worth considering.

Metal-detector wands are relatively inexpensive, and can be used by security personnel or other staff to check individuals for hidden weapons. Detection portals, which students can walk through, are much more expensive, and baggage x-ray machines can cost in the tens of thousands of dollars.

The effectiveness of metal-detection equipment has received mixed reviews for at least three reasons:

1. There are usually many entry points that students can use to bring weapons into the schools, including open windows or secondary doors.
2. Use of the equipment requires the staggering of students' arrival at school to allow sufficient time for processing.
3. The equipment cannot operate itself. At the very least, two security personnel must be hired to operate the wands: scanning incoming students, taking students aside who trigger the alarm, monitoring the remaining students, and responding to found weapons. Between the equipment and staffing, this can be a very expensive proposition.

One alternative is a free-standing metal-detection security portal. Visitors who enter the portal cannot gain further entry if metal is detected. Their only option is to leave or to communicate over an intercom, monitored by a camera. These devices are effective, but their cost, up to $80,000 per entry, is a major deterrent.

What Kinds of Alarm Systems Can Be Employed?

Alarms have two principal functions: They can detect intruders after hours or in controlled areas, and they can signal emergency personnel when immediate help is needed.

Alarm systems can be designed to automatically detect intruders, smoke, or flame. They can also allow staff to trigger "panic" buttons in emergencies, such as when a gunman is seen entering the building. In some circumstances, specific staff or students can be issued wireless pendants that serve as duress alarms. Technology can then be used to electronically pinpoint the pendant's location on campus.

Alarms can be triggered by a variety of devices, including motion detectors, glass breakage, and electrical contacts (triggered by the opening of doors or windows). Microphones incorporated into the system allow a

Tod Schneider is the Eugene (Oregon) Police Department's Crime Prevention Specialist and Crime Prevention Through Environmental Design (CPTED) Analyst. Email: tod@pond.net

monitoring station to hear what is being said inside the school and relay that information to police.

What Conditions Justify Installation of Surveillance Equipment?

Surveillance technologies are appropriate when (1) offenders need to be identified, and their actions documented; (2) hidden areas are attracting problem behaviors that have not been successfully deterred through other measures; and (3) the offenders may be students or staff members, with legal access to the school.

Surveillance equipment is a worthwhile investment when documentation of problem behavior and identification of suspects is important. All equipment should be field-tested before purchasing. Lighting conditions, focal length, equipment capabilities, and the weather can all have an impact on the quality of images generated.

Closed Circuit Television (CCTV) cameras' greatest strength lies in identifying suspects after the fact. They can also deter some criminal activity. But cameras are not foolproof. They may be targeted by vandals, so they must be installed with this possibility in mind. Premeditated crimes can be planned to avoid the cameras, or offenders can wear disguises to obscure identities.

Problem locations, such as specific bus routes or classrooms, can be brought back under control by advertising the installation of cameras, whether or not cameras are actually installed. One drawback to fake cameras is the possibility that students will assume they can rely on a certain level of security when in fact that is not the case. Cameras targeting dark areas may require Infrared (IR) capabilities.

Technical differences between cameras include the following basics:

Fixed versus moving (pan and tilt) cameras. Fixed cameras tend to require much less maintenance, and can be relied upon to catch the intended images. Moving cameras cover more areas, but require more maintenance and frequently miss critical details of an incident. One option is to integrate the camera into the duress-alarm system; the camera remains fixed unless an alarm is triggered, at which point the camera pans to the alarm location.

Wireless versus hardwired systems. The distance between a camera and a receiver will affect the quality of images received, even with hard-wired systems. Standard coaxial cabling will suffice for distances of up to 1,000 feet, but greater distances will require repeaters that pass along a wireless signal or fiber-optic cabling that can greatly expand the maximum distance covered by a hardwired system.

It is not realistic to expect staff to watch CCTV monitors to catch criminal behavior as it occurs. Studies twenty years ago by Sandia labs demonstrated that twenty minutes is about as long as an average human being can stay focused on this task. The monitors are primarily a tool for reviewing incidents after the fact.

Until recently, the standard technology for recording video images has been the use of videotapes (analog recording). A disadvantage is that tapes must be manually labeled and replaced every twenty-four hours as well as stored as evidence.

Videotaped recording is rapidly being overtaken by digital video recording (DVR) technology. DVR can retain voluminous records for long periods. The best systems have a "mean time between failure" rate (MTBF) of about 100,000 hours, and most have the ability to self-diagnose and correct problems, prompt users with software-generated alarms, and set off pagers or faxes to alert security staff. Analog images frequently render images so fuzzy as to be useless for identifying suspects, whereas digital technology gets sharper every year.

DVR technology can be integrated with access-control mechanisms, allowing users to pull up all images in certain locations where anyone has gained access during certain hours, all within minutes. The analog approach, in contrast, would require mind-numbing hours of viewing.

DVR technology can also take advantage of a local area network, allowing a school district's central office to pull up images from distant facilities.

What Factors Should a School Consider in Choosing Security Technology?

An important first step is to carefully identify the problem before investing in a solution. Technology can be seductive, but it isn't always the right tool for the job. Metal detectors and ID cards won't stop bullying behavior; security cameras won't stop intruders.

Cost-benefit analysis should be employed to compare this investment with other school needs. These should first be prioritized, then solutions should be sought. Personnel costs such as security guards, equipment maintenance, and upgrades should be considered over a ten- to twenty-year time frame for comparison purposes.

Technological shortcomings should also be considered. Particularly when schools turn to technology as a "quick fix," there is a high risk of reinforcing a climate of fear and distrust, undermining the social ecology of the school, instead of actually having an impact on the identified problem.

Technology can also turn out to be unwieldy or impractical. For example, metal detectors need to be staffed; who is going to do that? Will students be lined up for half a block every morning waiting to get in? Maintenance and repair concerns must be addressed; if it breaks on the weekend, who knows how to fix it? Where can spare parts be obtained? References should be checked. The best resources are other school districts that have already chosen vendors and technology. Learn from their successes and mistakes.

Ease of expansion, integration, and system upgrades should be considered. Finally, ask vendors about system flexibility as technology changes.

Resources

Green, Mary. *The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies*. Los Alamos, NM: Sandia National Laboratories, 1999, for the U.S. Department of Justice, NCJ178265. 282 pages. ED 436 943.

Schneider, Tod; Hill Walker; and Jeffrey Sprague. *Safe School Design: A Handbook for Educational Leaders—Applying the Principles of Crime Prevention Through Environmental Design.* Eugene, Oregon: ERIC Clearinghouse on Educational Management, University of Oregon, 2000. 111 pages.

Websites

American Society for Industrial Security (ASIS). www.asisonline.org

National Burglar and Fire Alarm Association. www.alarm.org

Security Products: The Integrated Product Newsmagazine for Security, Fire, and Safety Professionals. Stevens Publishing. www.secprodonline.com

A Product of the ERIC Clearinghouse on Educational Management • College of Education, University of Oregon • Eugene, Oregon 97403-5207

This publication was prepared with funding from the Office of Educational Research and Improvement, U.S. Department of Education, under contract No. ED-99-C0-0011. The ideas and opinions expressed in this Digest do not necessarily reflect the positions or policies of OERI, ED, or the Clearinghouse. This Digest is in the public domain and may be freely reproduced. The text of this Digest may be viewed electronically at **http://eric.uoregon.edu** EA 030 822.

.