

***Idaho State Department of Education  
Office of Safe & Drug-Free Schools***

***An Educator's Guide to School Safety Equipment***



# CONTENTS

<b>Introduction</b> .....	<b>3</b>
<b>Prelude</b> .....	<b>4</b>
<b>Chapter One: Overall Security Picture</b> .....	<b>5</b>
<b>Chapter Two: Video Surveillance</b> .....	<b>16</b>
Video Cameras	
Why video cameras	
Why NOT video cameras	
Good applications versus poor applications	
To monitor or not to monitor	
Color versus black-and-white cameras	
Fixed versus pan-tilt-zoom cameras	
Hardwired versus wireless systems	
A more technical discussion of formats, resolution, pixels, lenses, and field of view	
Camera housings	
Placement and mounting	
Lighting requirements and nighttime applications	
Covert cameras	
Maintenance and expected lifespan	
Price ranges	
<b>Video Recording Equipment</b> .....	<b>31</b>
VCRs/Time-lapse recorders the weak link	
Multiplexers	
Digital Video Recorders	
<b>Chapter Three: Detection Products</b> .....	<b>34</b>
<b>Walk-through Metal Detectors</b>	
Do metal detectors really work? – The Basics	
Space requirements and layout	
Throughput	
Hardware costs and manpower costs	
<b>Hand-Held Detection</b> .....	<b>38</b>
The name of the game: Policies and procedures	
Space requirements	
Throughput	
Hardware costs and manpower costs	
<b>Chapter Four: Entry-Control Technologies</b> .....	<b>42</b>
<b>Limiting Entry/Exit Points</b>	
<b>Entry-Control Approaches</b>	
WHO lets you in?	
What you HAVE	
What you KNOW	
Who you ARE	
<b>Chapter Five: Duress Alarm Devices &amp; Their Role in Crisis Management</b> .....	<b>48</b>

## INTRODUCTION

Creating a safe school environment is the responsibility of the entire community in which a school or school system is located. But on a day-to-day basis, the primary responsibility lies with school district officials and school administrators. To assist in this task, the Idaho State Department of Education has sponsored research and demonstration programs to collect data and test useful new ideas. The results will expand understanding of a school's preparation, mitigation, and response to critical incidents such as school violence, fire, or natural disasters, etc., and lead to the development of new programs to control these types of incidents.

This document provides a basic-level guide for school administrators. It encourages their collaboration with stakeholders as they decide which security technologies to consider in the development of their own safe school strategies. It is important to note that no single formula can possibly address every school or district within the state of Idaho and that individual plans must be tailored to the specific needs and capabilities of the given institution. This document is not designed to be an all-inclusive "how to" manual, but rather a guide for the purchase and procurement of security technology that will help you make the most beneficial decisions given your set of circumstances.

In the wake of recent high-profile school tragedies with multiple homicides, many of this nation's communities have urged their school districts to incorporate security technology into their safety programs. When used as a team approach in conjunction with solid crisis planning, this guide will help schools and their stakeholders analyze their vulnerability and suggest possible technologies to aid in addressing violence, theft, vandalism and other events that compromise student safety. This guide describes commercially-available technologies and urges thoughtful consideration of not only the potential safety benefits of a product, but also the costs that schools may incur for capital investments, site modifications, additional staffing, training, equipment maintenance, and repair.

This guide covers many topics including: security concepts, operational issues, video surveillance, weapons detection devices (walk-through and handheld weapon and or explosives detection), entry controls, and duress alarms. It offers practical guidance enabling schools to make better informed decisions about security technology. However it does not provide detailed instructions on installing equipment or making cost estimates, nor does it replace the use of an appropriate on-site expert.

It is imperative that school officials understand that safety and security technology is only one part of a comprehensive safety program.

## Prelude

With support from the Idaho Legislature, in August 2007 the Department of Education authorized The Safe and Secure Schools Assessment in Idaho. The assessment was completed in November 2007 and produced an accurate and comprehensive picture of the current security profile of Idaho schools. This independent assessment revealed some troubling information that must be addressed immediately. The current state of safety and security across Idaho K-12 public schools is inadequate, and is clearly a concern among administrators, staff and parents. The Safe and Secure Schools Assessment surveyed 520 school principals and 92 district superintendants across Idaho. Superintendants rated 85% of all Idaho schools as partially or fully inadequate in the safety and security they provide. These ratings were validated by data gathered through stakeholder surveys, site visits, public meetings, and interviews with school officials.

It is our intent to share what we have learned about the strengths and weaknesses of security technologies through our work with the security specialist. We have learned that school security, like other types of security, is not simple and straightforward. We have learned a lot about the unique aspects of school security from the many students, parents, school personnel, and law enforcement we met during the course of our work. A school's security program is the product of funding, facilities, building age, building layout, administrators, teachers, parents, kids, campus order, security personnel, policies, procedures, the neighborhood, the school board, local law enforcement, fire codes, local government, politics, and reputation. No two schools will have identical security programs—hence, a security solution for one school cannot just be replicated at other schools with complete success.

It became clear after working with more than 100 schools during 2007 that school administrators need a good resource for information on technologies for physical security problems. This guide is anticipated to be the first in a series of manuals designed and written for use by school administrators. This document provides nontechnical, vendor-neutral information on:

- Security products available on the market.
- The strengths and weaknesses of these products and their expected effectiveness in a school environment.
- The costs of these products, including installation, long-term operational and maintenance expenses, manpower, and training.
- Requirements to include in Requests for Quotes (RFQs) to specify the best product for an application.
- Legal issues that may need to be addressed.

Although security products can certainly have many different applications, this document covers products that can be applicable to some of the issues of school violence through video surveillance, weapon detection, entry control, and duress alarms. Future volumes are expected to cover issues and products such as bomb threats and explosives detection; drug residue and vapor detection; drug and alcohol use detection; interior and exterior intrusion detection sensors; alarm communications; false fire alarm pulls; glass-break sensors; two-way radios; fencing; antitheft property marking; doors, locks, and key control; Crime Prevention through Environmental Design principles; and parking lot safety. Most of the issues and philosophies covered in this manual are primarily aimed toward middle schools and high schools, but elementary schools may find several of the technologies to have possible applications at their facilities.

This guide is intended to provide an overview of security technology product areas that might be appropriate and affordable for school applications. Feedback from schools, law enforcement agencies, product manufacturers and vendors is welcome, especially regarding any oversights or errors on our part. Corrections or additions will be included in future updates. (Cost estimates for hardware may not reflect current pricing).

**CHAPTER ONE**  
**OVERALL SECURITY PICTURE**

Most schools in Idaho are safe institutions, with disciplinary issues creating most disruptions. However, because of the recent school violence involving students, firearms, and multiple victims, schools and school programs are working harder to reach out to students and to teach them to be good citizens, to identify potentially dangerous personalities, and to develop appropriate intervention strategies. There are many excellent programs around the country that address the issues of bullying, anger, hate, abuse, drugs, alcohol, gangs, lack of role models, vandalism, and so forth. It is of great importance to the State of Idaho that these programs be pursued expeditiously. Unfortunately, these programs cannot be successful overnight (indeed, many must be initiated early in a child's life in order to be most effective) and do not yet exist in all schools. Meanwhile, security incidents are occurring in schools that must be dealt with now—perpetrators must be caught and consequences must be administered. School administrators would like to discourage security infractions by means of any deterrent available to them. One such approach sought more often today involves security technologies.

Security technologies are not the answer to all school security problems. However, many security products (e.g., cameras, sensors) can be excellent tools if applied appropriately. They can provide school administrators and security officials with information that would not otherwise be available. They can be used to perform mundane tasks and free up manpower for more appropriate work. They can even save money (compared to the long-term cost of personnel or the financial impact of not preventing a particular incident). Too often, though, these technologies are not applied appropriately in schools. They are expected to do more than they are capable of or are not well maintained. In these cases, technologies are certainly not cost-effective.

### ***Why security technologies?***

In order to reduce crime and violence in schools:

- The opportunities for security infractions should be eliminated or made more difficult to accomplish.
- The likelihood of being caught must be greatly increased.
- Consequences must be established and enforced.

Establishing and enforcing consequences is a social and political issue and needs to be addressed head on by school boards and communities across Idaho. This guide addresses only the first two items.

Simply providing more adults, especially parents, in schools will reduce the opportunities for security infractions and increase the likelihood of being caught. However, adding dedicated professional security staff to perform very routine security functions has many limitations:

- Locating qualified people may be difficult.
- Humans do not do mundane tasks well.
- Manpower costs are always increasing.
- Turnover of security personnel can be detrimental to a security program.

As in other security environments, more repetitious tasks become boring. Hence, the possible role of security technologies expands. Through technology, a school can introduce ways to collect information or enforce procedures and rules that it would not be able to afford or rely on security personnel to do.

### ***Why security technologies have not been embraced by schools in the past?***

Anyone working in the security field is aware that there are thousands of security products on the market. Some of them are excellent, but many claim to be “the very best of its kind.” And unfortunately, there are a significant number of customers in the country who have been less than pleased with the ultimate cost, maintenance requirements, and effectiveness of security technologies they have purchased. Schools are no exception and have a few inherent problems of their own:

- Schools do not usually have the funding for aggressive and complete security programs.
- Schools generally lack the ability to procure effective security technology products and services at

- the lowest bid.
- Many school security programs cannot afford to hire well-trained security personnel.
  - School administrators and their staff rarely have training or experience in security technologies.
  - Schools have no infrastructures in place for maintaining or upgrading security devices—when something breaks, it is often difficult to have it repaired or replaced.
  - Issues of privacy and potential civil rights lawsuits may prohibit or complicate the use of some technologies.

The issues come down to applying security technologies in schools that are effective, affordable, and politically acceptable but still useful within these difficult constraints.

### ***Effectiveness –vs- Affordability –vs- Acceptability***

Effectiveness, affordability, and acceptability are difficult tradeoffs and, occasionally, a seemingly ineffective solution to a security problem is chosen because of a lack of funding or pressure from the community to do something. Although many effective security measures are too expensive for schools, cost alone is not often the ultimate driver. Most major changes to security policies, including the introduction of technologies, are often brought on not by foresight but as a response to some undesirable incident.

This is not to say that a good argument should be made for applying every physical security approach in every school. “Appropriate” preparation is by far, the greater “art” in security system design and it includes an evolving plan beginning with defining a particular school’s risks.

### ***A systematic approach to identifying the security risks at a school***

In the past, schools have rarely understood the need or had the time or resources to consider their security plans from a systems perspective—looking at the big picture of what they are trying to achieve in order to arrive at the optimal security strategy. A school’s security staff must understand what it is trying to protect (people and/or high-value assets), who it is trying to protect against (what the threats are), and the general environment and constraints (legal, moral, ethical as well as the mission of the school district) that it must work within—the characterization of the facility. This understanding allows a school to define its greatest and/or most likely risks so that its security strategy consciously addresses those risks. This strategy will likely include some combination of technologies, personnel, and procedures that do the best possible job of solving the school’s problems within its financial, logistical, and political constraints.

### ***Why is careful identification of risk important?***

You have to; neither because few facilities, especially schools, can not afford a security program that protects against all possible incidents nor could such a system realistically exist within a school and still maintains a sound educational environment. No two schools are alike and, therefore, there is no single approach to security that will work ideally for all schools. A school’s security strategy will need revising from year-to- year as the world around it and the people inside it are always changing.

### ***Defining a school’s asset***

For this school year, what is most at risk? The protection of the students and staff is always at the top of this list, but the measures taken to protect them will usually be driven by the defined threats. Are the instruments in the band hall attractive targets for theft or vandalism? Is the new computer lab full of the best and most easily resold computers? Though desirable, a school cannot possibly afford to protect everything to the same level of confidence.

### ***Defining threats in a school***

For this school year, who or what is your school threatened by?

Gang activity?

Fights behind the gym?

Drugs hidden in lockers?

Guns brought to school?

Unauthorized persons on campus?

Alcohol consumption at lunchtime?

Vehicle break-ins?

Graffiti?

Traffic accidents in the parking lot?

How sophisticated do the perpetrators seem to be (knowledgeable of their task of ill will)? How motivated do the perpetrators seem to be (willing to risk being caught or injured)? Measures taken to protect against these threats are driven by the characterization of the facility and its surroundings, as mentioned earlier.

### **Characterizing a school's environment:**

Any security strategy must incorporate the constraints of the facility so that all strengths, weaknesses, and idiosyncrasies are realized and provided for. How risks are approached will largely be driven by facility constraints. If theft and vandalism are primary risks for your school, answers to questions regarding the physical plant will determine the optimal security measures. Is the school new or old? Are the windows particularly vulnerable? Does everyone who ever worked at the school still have keys? What is the nighttime lighting like? Are gangs present in the area? Does the interior intrusion sensor system work well, or do the local police ignore the alarms due to a high false-alarm rate?

If outsiders on campus are a primary concern, it will be necessary to recognize the facility's ability to control unauthorized access. Are visitors forced or merely requested to go through the front office before accessing the rest of the school? How many entry points are there into the buildings? Are the school grounds open and accessible to anyone, or do fences or buildings restricting access? Is there easy access to the school roof? Where are hiding places within the building or on the premises? Is the student population small enough so that most of the staff would recognize most of the students and parents? Has the staff been trained to identify and report suspicious or unknown persons on campus to the proper person(s) on campus? Does the school staff have the support of the administration to confront suspicious or unknown persons?

If issues of violence are a major concern, a thorough understanding of employees, student profiles, and neighborhood characteristics will be necessary.

- What is the crime rate in the neighborhood?
- Is the school administration well liked by the students?
- Are teachers allowed access to the school at night?
- Are students allowed off campus at lunch time?
- How much spending money do students generally have?
- Are popular hangouts for young people close by and, for business establishments, does management collaborating with the school?
- Are expelled or suspended students sent home or to an alternative school?
- How many incidents of violence have occurred at the school in the past?
- What is the general reputation of the school, and how does it appear to an outsider?
- Are your most vocal parents pro security or pro privacy?
- Do your students like and respect your security personnel well enough to pass them pieces of information regarding security concerns?
- Are your security and administrative personnel trained to listen for rumors and to gather intelligence?
- Do they actively form partnerships with the school community as a whole to encourage the dissemination of information that may prevent violence?



Once the school's threats, assets, and environmental constraints are understood, the security needs can be prioritized such that the school's security goals are understood by all those involved. Identifying security needs and then securing the funding to pay for them are usually unrelated at most schools. Schools have to have a "Plan B," for program design which may be the perfect "Plan A"—but spread out over several years of implementation. If the desirable strategies (e.g., fencing, sensors, locker searches, speed bumps) are too costly or unpalatable to the community, a school may then need to modify the facility constraints (e.g., back entrances locked from the outside, no open campus for students, no teacher access after 10 p.m., all computer equipment bolted down, no lockers for students).

Most school districts or school boards will be more supportive of security measures and the requested funding if they are well educated about the most likely risks faced each year and the options available. A security staff should not have the wide-open charter to "keep everything and everybody safe." A school board should be briefed at least monthly as to the current security goals and what strategies are recommended, realizing that these will continue to evolve. This is a critical concept that must be grasped and acted upon in order to facilitate the justification and procurement of appropriate security technologies. School administrators and security personnel should develop a database to record all criminal and disciplinary actions as well as all threats that have been analyzed and responded to during any given school year. This statistical data will prove invaluable in assessing and prioritizing one's needs. If a school board member is clearly aware of a school's most important concerns and what is required to achieve them, then he or she is less likely to be swayed by an irate parent into making a decision that will handicap reasonable security efforts.

### ***Designing the school security system***

After identifying the risks or concerns at an educational facility, a methodical approach to the security plan would then examine possible solutions to each area of vulnerability from the perspective of:

**Deal with Denial**  
**Deter**  
**Detection**  
**Delay**  
**Response**  
**Consequence**

"Denial kills you physically, mentally, and financially. It has no survival value. Chew it up, spit it out, and get rid of it. (Moment of truth today, no more denial) rid yourself of every ounce." (Lt. Col Dave Grossman) basically overcome the mindset that this will never happen here to clear the way for effective security and safety planning). For any problem, it is necessary to detect that an incident or problem is occurring. For example, when someone is breaking into a building, it is necessary that this act be detected and that information be supplied to the authorities as soon as possible. Next, this adversary must be delayed as long as possible so that the response force may arrive. A simple example of delay would be firmly bolting computer components onto large heavy desks so that a thief is forced to use more time removing the bolts. Finally, someone such as the police must respond to the incident to catch the thief.

For a school environment, it is probably more appropriate to expand this model:

DETERRENCE	DETECTION	DELAY	RESPONSE/ INVESTIGATION	CONSEQUENCE
Signs	Security System	Access Control	SRO	Suspension
Cameras	Cameras	Fences	Video Playback	Expulsion
I.D Check	Hot Lines		Rewards	Citation
SRO	Staff			Arrest
Locker				Community Service
Search				
Vehicle				
Checks				
Drug Dog				
Fencing				

The most appealing step in any school security system should be to convince the perpetrator that he or she should not do whatever it is he or she is considering doing in the first place. It doesn't matter whether the action is perceived as too difficult, not worthwhile, or the chances of being caught are too high. Clearly, most security measures employed in facilities are intended for the precise purpose of deterrence, whether it is to discourage a thief, a drug dealer, or an errant employee. (Note: Deterrence is not generally considered part of the security strategy for most high-risk government facilities. This is due in part to the fact that quite a bit of deterrence comes "free" with other security measures, and it would be difficult to attribute a lack of security problems to any particular deterrence effort.)

Unlike other facilities, where a perpetrator would be handed over to the authorities, and the consequences determined by law, a school often has the authority and/or opportunity to establish the consequences for incidents that occur on their campus. It is imperative, however, that schools do not assume authority that they do not have. Issues governed by law must be reported to the appropriate authority.

To illustrate the application of this model, consider the problem of nighttime break-ins and theft in a school building. A model for the security strategy to address this might be:

**Deterrence:** Close off the parking lot or driveways to vehicle traffic at night. Post signs that video cameras are in use on the campus (only if you actually do have those cameras in use) and use fencing strategically.

**Detection:** Install an intrusion detection system in all school hallways, administrative offices, and rooms with high-value assets. Use motion sensors, magnetic switches on doors, heat sensors, and/or glass-break sensors as appropriate. Send alarm signals to the police, the officer on campus, and the school principal.

**Delay:** Secure high value assets as best as possible. An example would be bolting computers and TVs to desks and walls so that removing them is difficult and time consuming.

**Response:** Police and/or campus security arrives on the scene (investigation), makes arrests and follows through with prosecution (also a deterrent for future or potential offenders).

**Consequences:** Enforce consequences where possible and when the school has the authority to do so. (This becomes an additional deterrent, especially if non-sensitive pieces of information regarding the incident are released to staff, students, and the community.)

Since schools do not normally have the opportunity for real-time detection and response to security incidents, after-the-fact investigation is normally the best a school can hope for. Although this model may not be appropriate for all aspects of security at a school, it can serve as a methodology for consideration. Its use can prevent some less-thought-out strategies. Example: A high school was planning to purchase \$100,000 worth of exterior cameras to combat nighttime vandalism to the exterior of the building. This plan was halted abruptly when the school was asked who would be available to watch the monitors from the 40-plus cameras (detection) and who would be able to respond quickly enough to these sporadic and relatively small incidents (response). A better and cheaper alternate plan was devised that included indoor and outdoor motion lighting, strategically placed cameras, and more frequent police patrols.

### ***A spectrum of physical security approaches***

It is assumed that consequences for undesirable actions are in place at a school, otherwise there is little or no deterrence from any physical security measures designed to detect, delay, and respond to an incident. A wide array of security measures involving people, campus modifications, and/or technologies can be considered for most concerns, keeping in mind the unique characteristics of each school. A recurring message from school administrators is that the majority of their problems are brought onto campus by outsiders or expelled/ suspended students so measures to keep outsiders off campus will generally be of global benefit. School administrators quite often find it more palatable to parents when security measures are justified based on the exterior threat rather than the suspicion of their own children, although this is not the case in all incidents. The following is a partial list of possible security measures to address various security issues:

(Most of these security measures are used in one or more Idaho schools, but a few may not yet have been attempted. In any case, there is no comprehensive body of knowledge regarding their effectiveness. More research is needed to get a complete picture of particular technologies used in Idaho schools.)

#### ***Outsiders on campus***

- Posted signs regarding trespassing, video surveillance, visitors, trespassing, etc.
- Enclosed campus (fencing).
- Guard at main entry gate to campus.
- Greeters in strategic locations.
- Student I.D.s or badges.
- Vehicle parking stickers.
- Uniforms or dress codes.
- Exterior doors locked from the outside.
- A challenge procedure for anyone out of class.
- Cameras in remote locations.
- School laid out so all visitors must pass through front office.
- Temporary “fading” badges issued to all visitors.

#### ***Fights on campus***

- Cameras.
- Duress alarms.
- Whistles.

#### ***Vandalism***

- Graffiti-resistant sealers.
- Glass-break sensors.
- Aesthetically pleasing wall murals (these usually are not hit by graffiti).
- Law enforcement officers on campus.
- 8-foot fencing.
- Well-lit campus at night.

### ***Theft***

- Interior intrusion detection sensors.
- Property marking (including microdots) to deter theft.
- Bars on windows.
- Reinforced doors.
- Elimination of access points up to rooftops (exhibit 1.5).
- Cameras.
- Doors with hinge pins on secure side.
- Bolting down computers and TVs.
- Locating high-value assets in interior rooms.
- Key control.
- Biometric entry into rooms with high-value assets.
- Law enforcement officer on campus.

### ***Drugs***

- Drug detection swipes.
- Hair analysis kits for drug use detection (intended for parental application).
- Urinalysis drug detection kits (parental application)
- Detection K-9's.
- Removal of lockers.
- No backpack or bag policies
- Random searches.
- Vapor detection of drugs.

### ***Alcohol***

- No open campus at lunch.
- Breathe test equipment.
- Passive alcohol sensors
- No access to vehicles.
- No lockers.
- Clear or open mesh backpacks.
- Saliva test kits.

### ***Weapons***

- Walk-through metal detectors.
- Hand-held metal detectors.
- Vapor detection of gun powder.
- Crime stopper hotline with rewards for information.
- Gunpowder detection swipes.
- Random locker, backpack, and vehicle searches.
- X-ray inspection of book bags and purses.

### ***Malicious acts***

- Setback of all school buildings from vehicle areas
- Vehicle Standoff
- Inaccessibility of air intake and water source
- All adults on campus required to have a photographic ID badge.
- Vehicle barriers near main entries and student gathering areas.

### ***Parking lot problems***

- Cameras.
- Parking Permits (decals).
- Fencing.
- Card I.D. systems for parking lot entry.
- Barcode tracking system
- Parking lots sectioned off for different student schedules and or age levels.
- Sensors in parking areas that should have no access during school day.
- Roving guards.
- Bike patrol.

### ***False fire alarms***

- Sophisticated alarm systems that allow assessment of alarms (and cancellation if false) before they become audible.
- Boxes installed over alarm pulls that alarm locally (screamer boxes).

### ***Bomb threats***

- Caller I.D. on phone system.
- Bomb threat response training for staff
- Threat assessment team in place
- Crime stopper program with big rewards for information.
- Recording all phone calls, with a message regarding this at the beginning of each incoming call.
- All incoming calls routed through a district office.
- Phone company support.
- No pay phones on campus.
- Policy to extend the school year when plagued with bomb threats and subsequent evacuations.

### ***Bus problems***

- Video cameras and recorders within enclosures on buses.
- I.D.s required getting on school buses.
- Security aides on buses.
- Smaller buses.
- Duress alarm system or radios for bus drivers.

### ***Teacher safety***

- Duress alarms.
- Roving patrols.
- Classroom doors left open during class.
- Cameras in black boxes in classrooms.
- Controlled access to classroom areas.

### ***Legal issues***

Within each section of this guide, some legal issues have been noted regarding the use of various technologies. A reasonable approach to using any new security device would include checking with your legal organization, talking to schools in the area that have already implemented the measure, and inviting local law enforcement to come in to discuss the device's possible use. Although every possible ramification cannot be foreseen, it does help to be aware of issues that might be raised and to be aware of current thinking about ways to address each of these.

## ***Evaluating a school's security system design***

The staff assigned to handle security concerns should plan to meet on a regular basis for collaboration on new problems, needed changes to existing approaches, and the exchange of information and intelligence. New problems and proposed solutions may sometimes be presented (where appropriate) to school employees, the student council, the parent advisory group, the local police, or other schools in the area. Although including more people may lengthen the decision making process, making representatives of these groups a part of the security upgrade team for issues that would involve them will ensure buy-in. A side benefit will be that word will spread throughout the community that the school is taking active security measures, which will act as a deterrent.

## ***New school design***

Many school buildings in the United States have been constructed to achieve an inviting and open-feeling, with large windows, multiple entrances and exits, and many opportunities for privacy. Unfortunately, these layouts are not conducive to many current requirements to address security needs. To combat broken windows and nighttime thefts, the country saw a period of schools designed with almost no windows. The cave-like results these designs produced were soon found to be objectionable to many people.

If a district has the fortune of building a new school, it is imperative that trained security personnel familiar with the area and the community, and who will be responsible for day-to-day security operations in the new facility, be involved in the design from the beginning to ensure that the new school minimizes vulnerabilities. There are architectural firms specializing in schools that incorporate good security principles. A security-conscious design can actually help compensate in the long term for tight security budgets, fewer security personnel, and less sophisticated security gadgets. The following are some suggestions to keep in mind for a new facility. The funding, location, geography, streets, and neighborhood of each new school will usually drive which ideas are feasible.

This list includes only a few basic security technologies (such as cameras, sensors, and so forth); the facility design should not preclude their straightforward installation in the future.

- Limit the number of buildings—one building is best—to limit outsiders on the campus.
- Minimize the entrances to the school building—having one or two main entrances/exits will support efforts to keep outsiders off campus. Allow enough room at the main entry in the event that a screening area (i.e., for weapon or drug detection) needs to be incorporated later on. Alarm other exits for emergency use only.
- Minimize the line of sight from secluded off-campus sites onto student gathering areas, the main entry doors, playgrounds, patios, and so forth (This suggestion must be tempered against the benefits gained from the natural, desirable surveillance by neighbors, passers-by, officers on patrol, and so forth).
- Allow for a security person to be posted at a single entrance onto campus to challenge each vehicle for identification of all occupants. Buses and school employees should have a separate (and controlled) entrance.
- Provide a drop off/pickup lane for buses only.
- Minimize the number of driveways or parking lots that students will have to walk across to get to the school building.
- Build single-stall bathrooms to mitigate bathroom confrontations and problems.
- Enclose the campus. (This measure is more to keep outsiders out rather than to keep insiders in.) Besides defining property boundaries, a robust fence forces a perpetrator to consciously trespass, rather than allowing casual entry.
- Make certain that the school building and classroom areas can be closed and locked off from the gym and other facilities used during off hours.
- Minimize secluded hiding places for unauthorized persons, both inside and outside buildings.
- Do not eliminate windows, but use them strategically. Consider incorporating clerestories or secure skylights that allow light in but that are less vulnerable than typical windows.
- Maximize the line of sight within buildings.

- Large wide spaces, like hallways or commons, should have sufficient vertical dimension so space does not feel restrictive to students.
- Consider installing student lockers in classrooms or other areas easy to monitor so that there is no single locker area that becomes a bottleneck, and there is always the deterrence of an adult nearby.
- Do not cut corners on communications, especially those required for security. Make certain that your facility has built in the necessary receivers and transmitters throughout the structure to allow for dependable two-way radio and cellular phone use. (Sometimes radio frequency communication is not possible deep within a large, structurally-dense facility.)
- Where possible, have buildings and other student gathering areas set back from the streets, driveways, or parking areas by at least 50 feet.
- Install a basic security alarm system throughout all hallways, administrative offices, and rooms containing high-value property, such as computers, VCRs, shop equipment, laboratory supplies, and musical instruments.
- Provide a separate parking area for work-study students or those who will be leaving during the school day. (This allows the main student parking lot to be closed off during the school day.)
- Make certain that exterior lighting is sufficient for safety. Lights mounted on the exterior of buildings often are inadequate for adjoining driveways or parking lots.
- Do not underestimate the value of trees and landscaping on a school campus. An attractive, well-maintained school is generally less attractive to thieves.

### ***The role of order***

One additional consideration that should not be overlooked is the perception of a lack of order on a school campus. If a school is perceived as unsafe (i.e., it appears that no adult authority prevails on a campus), then “undesirables” will come in and the school will actually become unsafe. This is an embodiment of the broken window theory: one broken window left unrepaired will encourage additional windows to be broken. Seemingly small incidents or issues such as litter on a school campus can provide the groundwork for (or even just the reputation of) a problem school. Issues of vandalism and theft can be almost as harmful to a school as actual violence because they can create a fertile environment for loss of control and community confidence.

Issues contributing to a school’s overall order maintenance must therefore be taken seriously, not unlike any other public facility. Reducing theft, deterring vandalism and graffiti, keeping outsiders off campus, keeping the facility in good repair, maintaining good lighting and attractive landscaping, and getting rid of trash are all important to school security. Technologies such as cameras, sensors, microdots (for identifying ownership), and anti-graffiti sealers can contribute significantly in many (but not all) situations and are possible approaches to further support a school’s order maintenance.

Too often school districts undervalue the importance of reliable and conscientious maintenance, janitorial, and grounds keeping staff. Their ultimate contribution to the order maintenance of a school can be enormous. Additionally, the janitorial staff needs to be selected with almost the same care as the teaching staff because they have great access to and knowledge of a school facility. Contracting out this work without complete background checks of all workers can lead to many problems in the long run.

**CHAPTER TWO**

**VIDEO SURVEILLANCE**



## **Video cameras**

### ***Why video cameras?***

The peace of mind of both students and faculty at a school can often be quickly enhanced by the installation of video cameras as part of a closed circuit television (CCTV) system. This added peace of mind may result in even further-reaching effects on a campus than would be expected by the use of cameras alone. As mentioned in the introductory chapter, a sense of safety and authority will directly influence people's opinions and impressions, which will ultimately contribute to the overall order maintenance of a facility and how that facility is treated by occupants and outsiders. To the school personnel who must handle day-to-day security issues, the best thing about cameras is the deterrence factor they introduce to outsiders who do not belong on campus and to students and employees who do. Information regarding security measures, such as cameras at the local school, will generally spread through a community.

This type of reputation can make outsiders reconsider an unwelcome visit to the historically easy mark of the neighborhood—the school. It can be assumed that most kids are not going to step way out of bounds if they believe they will likely be caught, which is often possible through the appropriate application of cameras. In a school security system, the ideal goal should be to convince kids not to even attempt to do something that is unacceptable. Addressing an incident after it occurs is good, but not as good as if it had never happened. Once a perpetrator is caught, there is a chain of events involving confrontation, denial, parental involvement, consequences, and perhaps even the involvement of law enforcement and the legal system. School administrators will be forced to spend a great deal of time on the matter, and all participants will find the process distasteful.

Strength of cameras is the evidence they can preserve on tape, CD, and DVD's. Even if law enforcement is not brought in regarding an incident, a tape recording, CD or DVD can be invaluable to a school administration. Many schools report that when students are brought into the school office after an incident and shown a tape, CD or DVD of them in an illegal or unacceptable act—even if the tape, CD or DVD might not have been of sufficient resolution and detail to use for prosecution purposes in a court of law—the student will usually admit to the incident.

The ultimate usability of a video recording is dependent on many variables. It is possible for a camera system to produce tapes on which individuals are unidentifiable or their actions are indiscernible. Be certain that a camera system provides the kind of information you need before you pay for it. These requirements should be clearly spelled out in the purchase agreement, along with a specified time period during which the school can adequately test it.

Video recordings are also beneficial for use with parents. Although nearly all parents want to believe their children are innocent of wrongdoing, some parents will deny their child's guilt despite the credible testimony of others to the contrary. However, as many school administrators and teachers have discovered, parents quickly accept their child's role in an incident when shown a videotape of the incident. Most parents want to do the right thing, but hard evidence is often required for some to concede over a matter involving their own child.

From a cost standpoint, the use of CCTV in public areas and on school grounds can free up manpower. If cameras are covering a large patio area where students congregate during breaks, adults who normally would be assigned to oversee that area can instead be made available to monitor other areas of concern.

Finally, the solid documentation that a video recording provides can be invaluable in situations involving liability claims. Although it is possible that this may occasionally work against a school, most schools welcome this concrete evidence so that testimony regarding an incident does not consist solely of hearsay.

### ***Why not video cameras?***

- CCTV systems are expensive. Installation can also be expensive, as well as logistically difficult.
- Choosing the correct camera equipment requires some technical knowledge.
- A single camera can effectively view a smaller area than would be intuitively expected, hence many applications can require more cameras, equipment, and expense than was originally expected.
- Cameras can be stolen or vandalized.
- Ongoing maintenance and operational support are required.
- Some applications or areas do not warrant camera use.
- Some communities or individuals will challenge the legality of using cameras.
- Insiders with full knowledge of the installed video system's capabilities can possibly circumvent the system to their advantage.
- If it becomes well known where cameras are being used at a school, students may simply move their misbehaviors to a different part of campus.

### ***Good applications versus poor applications***

An effective use of cameras is viewing the recorded tape, CD or DVD after an incident occurs. Examples of reasonable goals for a school video system are capturing scenes indicating who started a fight in the hallway, who is smoking marijuana in the parking lot, who stole the blank computer disks out of the computer laboratory, or if a particular person did indeed try to run down someone with his or her vehicle in the school driveway. Less reasonable goals, or at least more difficult or manpower intensive, are trying to use camera scenes to stop a student fight in its early stages, preventing someone from bringing weapons into the facility, or catching a thief before he makes his escape.

A visible camera may not help if a school's goal is to identify a nighttime thief in the band hall or computer lab if the thief simply covered his or her face or disguised him or herself. However, it may still add substantial deterrence when a would-be thief can never be sure if there will be some type of immediate response to the video recording or exactly where all the cameras are located.

Depending upon each situation, video cameras can support security initiatives in the following applications:

- School Stores.
- Computer Rooms.
- Science Laboratories.
- Cafeterias.
- Hallways.
- Supply Closets.
- Gymnasiums.
- Parking lots and driveways.
- Main administrative offices.
- Patio and entry areas.

Schools may want to consider classroom installation of the cameras and recorder enclosures that are currently so popular for use on school buses. On buses, a camera is placed in the black box only when requested by a bus driver, thereby reducing the number of camera systems that must be purchased. Usually, the deterrence factor derived from students never knowing when a camera is actually present can discourage much of the misbehavior. (This is not to be confused with the use of a dummy camera, where a potential victim is under the illusion that he or she is being monitored and, therefore, help will be forthcoming in the event of an attack. This can create extensive liability concerns for a facility.)

In an application with a camera looking in an easterly or westerly direction, extreme glare may occur during sunrise or sunset. If this type of placement cannot be avoided, the camera should be mounted as high as possible and then angled downward to view below the horizon. If sunrise and/or sunset are not critical time

periods for a particular application, then it may be acceptable to simply have an unusable picture during these times.

Viewing a scene such as a dark doorway that contains a significant shadow can be quite difficult. Similarly, vehicle headlights and other sources of glaring light, particularly during night operations, should be considered and compensated for. It is much more difficult to compensate for these problems after initial installation is complete. Oftentimes, funding is no longer available to make needed adjustments. Newer cameras with better electronics help compensate for these types of applications, but they are more expensive.

Seasonal problems should be anticipated and addressed before purchasing an exterior camera system. Conditions to be aware of are blowing snow, built-up ice on camera housing, dust storms, trees that block the scene in summer, temperature extremes, or north sides of buildings with shadows that may affect scene assessment during winter months.

### ***To monitor or not to monitor***

Each year, a great number of camera systems are bought in the United States with the objective of assigning a security person to constantly monitor the cameras in real time. The intent is that by having a live person watching the monitor, some sort of response may then be dispatched immediately and an undesirable incident prevented or stopped. This is quite often an unrealistic approach to security, particularly in school applications.

Experiments have been run to test the effectiveness of an individual whose task was to sit in front of a video monitor(s) for several hours a day and watch for particular events. These studies demonstrated that such a task, even when assigned to a person who is dedicated and well-intentioned, will not support an effective security system. After only 20 minutes of watching and evaluating monitor screens, the attention of most individuals has degenerated to well below acceptable levels. Monitoring video screens is both boring and mesmerizing. There is no intellectually engaging stimuli, such as when watching a television program. This is particularly true if a staff member is asked to watch multiple monitors, with scenes of teenagers milling about in various hallways, in an attempt to watch for security incidents.

A practical security application of real-time viewing of a video monitor might be the intent to actively allow or disallow individuals to enter a particular locked door. In monitors receives an alarm or other announcement that a person desires entry into that facility or area. The security person would then focus his or her attention directly on the screen and make a decision (according to procedures) as to whether to release the remote lock (if applicable) on a door to allow the person access.

Most schools have a security staff, whether it is an assistant principal assigned security as one of his or her duties, a few security aides equipped with two-way radios, or an impressive number of sworn police officers. Few schools, however, find themselves with surplus security-staff time.

Because of the ineffectiveness of people monitoring video scenes in real time, it would seem to be a very poor use of school security staff. One possible exception is when a certain incident is expected at a school during a finite time period. For example, if cars in a parking lot are frequently broken into during the noon hour, security staff may want to actively monitor their cameras' outputs during this period so that they may immediately assess an incident in progress and apprehend the suspect. This would be particularly appropriate if the suspect is not known and not a member of the school.

The use of cameras and a real-time display unit without the benefit of a recorder is not recommended. It is true that a video camera and monitor alone are much cheaper than a complete video system with recording and multiplexing capabilities. However, the hard evidence made available in the form of a video recording can more than make up for the cost of a recording system. Ease of prosecution and the likely prevention of future incidents by this individual are additional benefits.

### ***Color versus black-and-white cameras***

In a high-security application, when an alarm has been generated signaling a presence in an off-limits area, it is likely to be sufficient to be able to assess the alarm condition with a black-and-white camera. The objective here is merely to determine that it is a person (any person) intruding and that a response should be prepared or dispatched. In a school application, the security objective of recording video scenes would generally be to determine who the perpetrator of an incident was. In this type of after-the-fact assessment, it is most important to identify, not just detect, the intruder. Because of this, color cameras are probably more helpful for most school applications than black-and-white cameras.

Color recordings contain much more information about the scene that was viewed, i.e., the boy who broke the window had red hair, a dark yellow jacket, and drove away in a light blue car. This can be critical for school applications. The school principal can match the characteristics of the recorded suspect with those of students or outsiders known to frequent the area. Quite often, when a suspected student is brought in and shown a recording of him or herself in an incident, he or she will admit to a role in it, even though there may not have been quite enough detail on tape for a positive identification. Color cameras usually have lower resolution than black and-white cameras. However, for the school application, the ability to recognize the color of clothing, color of vehicle, and so forth is often more important than a more detailed image. The amount of information on a video recording that is required to prosecute a suspect in a court of law may be much greater in many instances than what a school video system will normally collect.

The cost of color cameras is slowly approaching the cost of black-and-white cameras. Currently, the cost of a color camera as compared to an equivalent black and-white camera is anywhere from 30 percent to 70 percent greater. Most school applications will find the higher priced color cameras necessary for their goals. An exception to this would be a camera applied in a small interior room or area where any potential perpetrators will be close enough so that their faces will be easily identifiable in black and white.

When using either black-and-white or color cameras under low light level conditions (such as at night with artificial lighting) it is necessary to evaluate the effectiveness of the existing lighting. Generally, security applications of cameras require higher light levels and more evenly distributed lighting than is found in parking lots with typical safety lighting. Also, if school officials plan to use their cameras for nighttime applications, color cameras will require a higher lighting level than black and white cameras.

### ***Fixed versus pan-tilt-zoom cameras***

Two types of camera configurations are available on the market: the fixed camera and the pan-tilt-zoom camera. Fixed cameras are mounted in a stationary position (although what the camera is mounted on may actually move, such as on a police vehicle). These cameras will view the same scene until physically relocated. The scene is typically recorded and, less often, the scene is also viewed simultaneously on a monitor by security personnel.

Pan-tilt-zoom cameras can operate in either of two modes. The mode for which these cameras are most useful allows the scene that is viewed to be controlled by an operator sitting at a video monitor. This operator can control the direction and angle of the camera as necessary. These cameras typically have a zoom option that will allow the operator to focus on parts of a scene, such as zooming in on a suspected perpetrator. The second mode for pan-tilt-zoom cameras is an automatic mode, in which the camera automatically scans back and forth over a certain portion of its range. Normally a pan-tilt-zoom camera should be protected and shielded from view by an opaque enclosure (domes are quite common) so that it is difficult for a would-be perpetrator to tell where the camera is actually aimed.

Most applications in schools are better served by fixed cameras. One consideration is that the pan-tilt-zoom camera can cost around three to five times as much as an equal quality fixed camera. More important though, is the fact that pan-tilt-zoom cameras run by an operator consume the time of a security staff member. When run in automatic mode, the chance of the pan-tilt-zoom camera looking (and recording) in the direction where an incident is occurring is much less likely than the chance it will be pointed in the wrong

direction. Pan-tilt-zoom cameras also introduce a mechanical component to the system that will require regular maintenance (e.g., oiling gears, replacing motors) and that may even fail.

Pan-tilt-zoom cameras may be employed during a fixed portion of the day, such as the lunch period, if an operator is available to watch and track suspects. Some high schools have a dozen fixed cameras located throughout the campus and successfully use one pan tilt-zoom camera to oversee the parking lot, allowing an operator to watch suspected perpetrators before and after classes. The goal is to record a suspected individual while he or she is involved in a regularly occurring incident of which the school is already quite aware. With these considerations, it would usually be more cost-effective and more reliable to capture incidents using multiple fixed cameras looking in different areas from a single point than to use a single pan-tilt-zoom camera. (This does not take into account installation costs.)

### ***Hardwired versus wireless systems***

Traditionally, camera systems have cabling that runs directly between the camera and the recording mechanism (or viewing monitor). These hardwired runs are usually recommended by manufacturers to not exceed 500–1,000 feet, using RG–59 coaxial cable. Signal equalizers/amplifiers will be required to compensate for signal loss if distances become much greater than 1,000 feet.

For exterior applications, cabling for camera systems should be placed within a watertight conduit. Underground cabling should be buried below the frost line or a minimum of 24 inches deep. Direct buried cables without conduit are subject to damage by rodents (if no rodent shield is provided), accidental digging, and intentional tampering. Above-ground cabling that is not in a conduit is very susceptible to tampering, as well as environmental degradation. With coaxial cable runs, ground loops (in video applications, this is a current flowing along the shield of the coaxial cable due to a voltage difference in the ground between the ends of the cable) and interference from radio frequencies (RF) or other signals must be considered. Coaxial cables should not be run next to, or parallel with, power lines over long distances. Equipment, such as transformers and electronic video clamps, is available in instances where interference is a problem.

With exterior coaxial cable runs, close lightning strikes can induce voltage surges on the cable that can damage equipment on both ends. To protect equipment, surge protectors are installed at both ends of the cable run.

Fiber optic cabling is an excellent alternative to coaxial cable. With fiber optics, there are no concerns with noise, RF interference, ground loops, or voltage surges. Fiber optic systems require a transmitter at the camera end and a receiver at the monitoring end. Fiber optic systems are more costly than coaxial cable systems for short runs but become more cost effective with longer cable runs (greater than 3,000 feet). Installation of fiber optics is also more expensive, requiring trained and experienced installers and specialized tools for handling and connecting.

For interior applications, cabling for hardwired camera systems should be placed within a metal conduit if it is exposed or accessible by building occupants, including maintenance staff. A good example of this is cabling run above loose, replaceable ceiling tiles. Short-distance, low-power RF wireless camera systems for video signal transmission are becoming more popular. (Wiring is still required for power.) A transmitter is required at the camera as well as a receiver at the recording end. This will add an estimated \$1,000 or more to the price of the system for each distinct camera location. Multiple cameras can be at one location. In many cases, however, wireless may be cheaper and certainly easier than running cabling.

Acceptable distances between a transmitter and receiver may range up to 1,500 feet if the camera transmitter is in direct line-of-sight of the receiver. If equipment is located such that data transmissions must go through walls, fences, and so forth, the detail of the transmission can quickly degrade if the transmitter/receiver distance is already close to the manufacturer's recommended maximum distance. Installation distances to be implemented for camera transmissions should be much less than manufacturer recommendations if the transmitter and receiver are not within each other's line of sight.

The advantage of wireless camera systems is that cabling does not have to be run underground, through the air, or behind walls and ceilings. Therefore, the chance of tampering is much less. However, wireless applications where distances are close to manufacturer limitations may experience interference from very unusual sources, e.g., a nearby parked truck. Previous installation experience is usually required to set up such a system, due to the different antennas available that can perform differently in unique setups.

Short-distance, low-power RF transmission systems, such as a school's wireless camera system, usually does not require licensing by the Federal Communications Commission (FCC). Higher power systems will require an FCC license.

***A more technical discussion of formats, resolution, pixels, lenses, and field of view:***

A basic familiarity with camera terminology is probably adequate for most school administrators who plan to go out on bid for a CCTV system. However, for the benefit of those who might be responsible for choosing or upgrading camera equipment, the following discussion presents these technical specifications in more depth.

**Formats:** Camera format relates to the size of the camera imaging device. Most solid-state cameras used in security applications today are 1/2-inch or 1/3-inch format. There are some 2/3-inch cameras still in use, and some 1/4-inch format cameras are beginning to appear on the market. The trend has been to make camera formats smaller as picture element densities have increased, giving the manufacturer more imaging devices per production run, reducing costs, and allowing for smaller cameras.

**Resolution:** Resolution is the ability to resolve or see small details in an image. Resolution for CCTV cameras (as well as for TV monitors and recorders) is usually specified in terms of horizontal lines of resolution. Horizontal lines of resolution relates to the number of independently resolvable elements (small details) in three-fourths of the picture width. CCTV cameras range from 200 to more than 1,000 lines of horizontal resolution. Higher resolution cameras generally cost more than lower resolution cameras. For a typical color security camera system (includes camera, cabling, recorder, and TV monitor) that uses a standard National Television Systems Committee (NTSC) color video signal format, 300 to 520 lines of horizontal resolution are common. Black-and-white systems for tighter security applications typically range from 500 to 700 lines of resolution. Cameras with more than 800 lines of resolution are commonly used in broadcast TV, medical, or industrial applications.

**Pixels:** An active picture element, sometimes referred to as pixels, is a term used specifically with cameras and is directly related to horizontal lines of resolution. Active picture elements are the actual number of light-sensitive elements that are within the camera imaging device. Active picture elements are expressed with a horizontal number (the number of elements horizontally across the imager device) and a vertical number (the number of elements vertically on the imager). A camera specified with 768H by 494V picture elements has 494 rows of picture elements vertically, with each row having 768 elements horizontally. For black-and-white cameras, horizontal lines of resolution relate to picture elements by a three-fourths factor (by definition of horizontal lines of resolution) so a black-and-white camera with 768 active picture elements will have 576 horizontal lines of resolution. This would hold true for color cameras as well, except that the NTSC format limits signal bandwidth which reduces resolution. Lines of resolution, camera format, and lens focal length (discussed later) are the camera-specific part of what determines if a camera scene will be useful for a particular application. Other items to consider include lighting, shadowing, camera aiming, and camera sensitivity. Before selecting a camera and lens combination for an application, one must determine what is desired to be seen in the image. Just being able to see a person in a specific area, such as a parking lot, will require one set of minimum criteria for camera and lens selection. Being able to identify a person by facial features (if the person faces the camera) will require a different set because a camera scene is observed on the TV monitor, the entire CCTV system resolution must be considered. This includes the camera and lens combination, the camera signal transmission equipment (such as coaxial cable and amplifiers), the TV monitor, and the recorder. All components of the system must have adequate resolution for the application desired.

For observation of a camera scene to determine only if a human is in the scene (or to be able to distinguish between a person and an animal), a minimum criteria of 5 horizontal TV lines across a 1-foot-wide object within the scene is used. (In terms of active picture elements, this means that a 1-foot-wide object would cover 8 horizontal active picture elements for each row of picture elements for the height of the object on the camera imager.) For identification of a person by facial features, 16 horizontal lines (21 pixels) of resolution subtending a 1-foot-wide object are needed.

The lens focal length (discussed in the next section), camera format, and how far an object is from the camera will determine how large an object is within the scene, as well as how many active picture elements the object covers on the camera imaging device. Higher resolution cameras (for example, 576 horizontal lines or higher) can be used to distinguish objects farther away (smaller in the scene) than a lower resolution camera (approximately 250 horizontal lines) allows. In other words, an object can be smaller in the scene for higher resolution cameras and still meet the minimum hour Lenses. A camera lens focuses light reflected from objects within a scene onto the imaging device of the camera. The imaging device converts light to an electrical signal. Lens focal length and aperture are two important parameters to consider.

Lens focal length describes the relative magnification of the lens. The camera field of view (defined below) will be dependent on the lens focal length, along with the camera imager format size. Similar to the camera imager format, there is a format size for lenses. For most cases, the lens format size should be matched to the camera imager format size. Mismatched format sizes can result in the focused image being too large or too small for the camera imaging device. Different camera and lens formats can be used satisfactorily in a few instances.

Except for the most uncommon sizes, there usually is not a large price difference between various lens sizes. The most common sizes are 4.8mm, 5.6mm, 8mm, 12mm, 16mm, 25mm, and 35mm. A 35mm lens has the longest range with the narrowest field of view. The 4.8mm lens can see much shorter distances, but it will have a much wider field of view. Most lens sizes can be used in exterior applications, depending on the view desired. Shorter focal length lenses, such as 4.8mm or 5.6mm, are typical for interior applications, due to the shorter distances involved.

The important thing to consider is that the camera field of view depends on the focal length and format size. Camera field of view is expressed in horizontal and vertical angular fields of view. Most camera manufacturers or manufacturers' representatives who sell lenses with their cameras can provide charts that list the angular fields of view for common lens sizes.

The lens aperture, or speed of a lens, is a relative measure of the ability of the lens to gather light. Aperture is expressed as the F-number. The F-number is the ratio of lens focal length to its clear aperture. Clear aperture is the diameter of the inside of the lens where light passes through when the lens iris is fully open. A lens that is designated as an F/2 will have a clear aperture size that is one-half its focal length, meaning that a 16mm focal length lens will have a clear aperture of 8mm. The lower the F-number of a lens, the lighter the lens can gather. This becomes important when operating a camera at low light levels, such as at night with artificial lighting. Most security camera lenses today have F-numbers of 1.8 to 1.4. These are usually adequate for night applications given that the minimum light levels for CCTV are provided. Not all lenses are the same, however. Two different lenses with the same F-number can have different light-gathering capabilities. This is particularly true when it comes to fixed focal length lenses versus variable focal length (zoom) lenses. Zoom lenses have more glass elements than fixed focal length lenses. Because of the additional glass elements, an F/1.8 zoom lens will not be able to pass as much light as an F/1.8 fixed lens with fewer glass elements. An amount of light transmission is lost in each glass element. This is important to consider during night operation under artificial lighting. A zoom lens will require higher lighting levels than a fixed focal length lens if an equivalent picture quality is desired.

Most lenses for security cameras will have an adjustable iris to control the amount of light that is received at the camera imager. The iris is either manually adjustable or electronically controlled. The electronic iris (or auto-iris) monitors the camera video signal output and will open the iris for decreasing light levels and close

it for increasing light levels. This keeps the video level (brightness and contrast) fairly constant under varying lighting conditions. In the case of a manual iris lens, the user or installer adjusts the iris opening for the proper video signal level for the expected operational lighting level. If light levels change, an adjustment to the iris will be required in order to maintain a proper video signal level. Manual iris lenses are used mostly in interior applications where no outside light comes in and the light levels remain constant. For all exterior and many interior applications, an auto-iris lens will be necessary.

A relatively new feature in many cameras is the electronic shutter. The electronic shutter is part of the imaging device and can perform close to the same function as an electronic iris. It controls the amount of light that the light-sensitive elements within the camera imager receive. Electronic shutters have limitations, however. They may not have as much range as auto-iris lenses. This is an important consideration for exterior applications. If light control is totally dependent on a shutter (a manual iris lens is used instead of an auto-iris) in an exterior application, the shutter may not be able to reduce light enough on bright, sunny days, resulting in portions of the picture washing out. If the manual iris lens is partially closed to compensate for bright sunshine, low-light conditions may produce a dark, noisy picture. Many shuttered cameras intended for exterior use will also come with an auto-iris lens.

A viewfinder can also be used to determine the field of view of a lens. This is a specially designed lens through which one can view the scene of interest. The scene is masked through the lens in such a way as to represent the picture that will be seen on the monitor. The scene desired can be dialed up on the viewfinder and the focal length of the lens required for the particular imager format size of the camera read from the side of the viewfinder. A viewfinder only determines a lens focal length value; other parameters must still be calculated.

Some lens manufacturers have developed tables for determining the field of view. The format size and focal length of the camera is cross-referenced to the column of the desired distance, and the width/height of the field of view is read from that column.

In summary, whether a camera scene is useful depends on whether objects can be distinguished in the scene. Camera resolution, camera format size, lens focal length, as well as lighting, shadowing, camera aiming, and camera sensitivity all play a role in being able to distinguish objects. Resolution and performance of other components such as TV monitors, recorders, and signal transmission equipment must be considered also. Cameras are specified with the number of horizontal lines of resolution and active picture elements; security cameras available today range from 300 to 700 horizontal lines of resolution. Black-and-white security cameras commonly have a horizontal resolution of 500 to 600 lines, while color cameras for security applications have 300 to 540 lines.

### ***Camera housings***

One of the first considerations in selecting camera housing is the environment. Is the camera to be installed outdoors or indoors? For indoor housings, the overall conditions where the camera is to be installed must be considered. Is the camera to be installed in a classroom, pool area, gymnasium, hallway, lobby area, or inside a school bus? A camera housing design can either help or hinder the installation and maintenance of a camera. In the outdoors, a watertight housing is desired; in some areas a heater may be required. Good ventilation is required in warmer climates. Domed enclosures are a special version of housings that can be used to conceal the position of the camera(s) via the use of viewing windows and various liners. The dome housing may also offer a more attractive look that can be designed to blend into its environment.

When installing housings in areas that drop below 30°F, the housing should have a heater. This is not so much to keep the camera warm as it is to protect the lens and to keep the view plate free from condensation. Many auto-iris and zoom lenses can begin to experience mechanical problems at temperatures close to and below freezing. For this reason, the housing heater should be located toward the front of the housing, preferably in a U-shape or circle around the lens area. This will keep the lens warm and the front faceplate clear. The camera itself will provide ample heat (under most conditions) to keep it operational. Check the specifications listing for the camera are operating temperatures. In extremely cold environments, it may be



necessary to purchase a housing that is also insulated. Extremely cold environments would be any location where temperatures drop to less than -30°F. A sunshield may be required in some locations. A sunshield can provide artificial shade and serve as a glare screen. A sunshield can lower the internal temperature of housing by 10–15°F and can reduce the effects of sunrise/sunset glare. Dome housings, because of their overall design, do not usually have a sunshield option.

In warmer climates, housing ventilation may be required. Many housings or domes have an optional fan attachment and air vents. Filters over the vents will need to be cleaned or replaced on a regular basis, thus adding to maintenance requirements. Sealed housings with fans for heat dissipation or condensation control can be used, but are usually more expensive.

Humidity can do the most damage to cameras and other electronic equipment. If the camera is to be installed in an obviously high-humidity area, a pressurized environmental housing may be required. These are purged and pressurized with dry nitrogen. The sealed pressurized housing ensures that changing outside pressures will not force any dirt, humidity, and/or oxygen into the tube. Cabling for these units is installed through the back via a specialized plug.

Corrosion caused by salt can be a major problem in areas of the country with high humidity that is near an ocean (such as California and Florida). Chlorine is a problem in pool areas. These different types of corrosives can dramatically reduce the life expectancy of a camera or lens. Therefore, if an environment is considered corrosive, only housings or domes that are considered environmentally sealed should be used.

A camera's vulnerability to vandalism must be taken into consideration. A housing or dome that can accommodate a lock may be required. To prevent tampering, the housing should be made of steel, although fairly tough plastic housings are available. Such tamper-proof housings or domes are often made of 10-gauge (or higher) steel. Some situations call for bullet-resistant housings. These units are usually constructed of 12-gauge stainless steel. The front glass will be constructed of a 1/4-inch or thicker Lean-type material. Two squares of 1/4-inch plate glass sandwiched around a 1/4-inch square of Lean can probably prevent scratching of the surface due to washing, wind, and dust.

When choosing a proper housing or dome, it is important to consider the actual dimensions of the unit. Refer to the camera and lens specification sheets to determine the size of the housing. Leave enough room for cable connectors. The objective is to keep the unit small but allow room for everything to fit and to be accessible. Ideally, the selected housing will allow the camera to be focused and the parameters adjusted while the camera is mounted inside the housing. This depends on the design of the housing. Some housing has a hinged cover, opening from the top that allows for easy focusing and adjustment. If mounted inside near the ceiling, this type of housing may not be feasible. Some housing allows the cover to slide off the base for easy adjustment of the camera parameters.

The prices of camera housings vary considerably. When going out on bid, be certain that your requirements document includes the features you will need.

### ***Placement and mounting***

To avoid the effects of blooming, streaking, and glare, all of which can wash out the video image, exterior cameras should be mounted below the nighttime lighting sources and aimed downward to shun direct sunlight, especially that occurring during sunrise and sunset. This may require a minimum mounting height of 18–20 feet. An even higher mounting height will help prevent vandalism of the camera. Consider the height required if a truck can be parked directly beneath the camera, where a perpetrator could stand on the truck's cab to reach the camera. Cameras should always be mounted on solid surfaces to prevent wind movement and vibration. Wooden, metal poles can twist with high winds over a period of time and cause the camera view to change. Under these conditions, the camera may periodically require direction alignment.

In the interior environment, cameras cannot be mounted higher than the ceiling so it may be easier for an intruder out-of-view of the cameras to vandalize or tamper with them. This situation can be helped if the scene viewed by two cameras includes the other camera, such as cameras mounted at each end of a hallway or room and aimed to include a view of the other.

Cabling to the cameras must be protected from vandalism and tampering. In interior installations, wires can be hidden from view and therefore protected by routing them through the ceiling and/or walls. However, the small amount of wiring that may run from the camera to the wall or ceiling must be in a conduit. Also be aware that employees with access to the ceiling could tamper with your camera wiring. For exterior camera installations, the video and power cabling to the cameras should be installed in a conduit. For underground runs, special cabling for direct burial should be used if the cable is not installed in a conduit. The cable running up poles or buildings to the cameras must be in a conduit because this is a very vulnerable location for vandalism and tampering.

Camera mounts should be selected to handle the weight of the camera, lens, and housing. A good rule of thumb is to select a mount that will handle twice the weight of the load as calculated from the specification sheets of the selected components. Mounts are usually specified as indoor or outdoor mounts. A mount designated for installation outside also can be used for interior installations, but an indoor mount should not be used outdoors. Outdoor mounts are treated for corrosive effects not normally encountered indoors (although one common exception would be in a high-humidity area such as an indoor pool). Some mounts have separate mounting bases and must be selected for either suspended ceiling or solid wall/ceiling mounting locations. Pole mount brackets are available for some outdoor camera mounts. The mounts should have adjustable heads to allow for up/down and sideways adjustment of the camera field of view. Mounts also come in different lengths, and this may be a consideration when camera housing adds to the length requirement. Primarily, the mount should be rigid enough and mounted securely enough to the surface so that the camera does not vibrate under normal operating conditions.

Many camera manufacturers and distributors also carry a full line of camera mounts, as well as housings for their cameras. Mounts are priced anywhere from approximately \$15 to \$150.

### ***Lighting requirements and nighttime applications***

Most schools generally will not attempt to use exterior CCTV cameras during the nighttime because of the high light levels that are required. For exterior nighttime CCTV applications, proper lighting is very important. A number of lighting types are available. These types include incandescent, fluorescent, and high-intensity discharge. Incandescent lighting is the most expensive to operate and includes the flood or quartz lights that are commonly used for exterior home security applications. Most fluorescent lighting is used indoors for office and work area lighting. High-intensity discharge lighting is the least expensive to operate (more light is produced with less power consumption) and is the most common for commercial exterior lighting applications. It includes high-pressure sodium and low-pressure sodium lighting. A disadvantage of high-intensity discharge lighting is the re-strike time. If a momentary power outage occurs, these lights will go out and can take up to several minutes to return to full brightness. The advantages of high- and low-pressure sodium lighting, however, outweigh this disadvantage for CCTV applications.

Low-pressure sodium lighting is the most desirable choice for exterior CCTV applications because it is somewhat more efficient to operate than high-pressure sodium, and the types of light fixtures available provide a fairly uniform light pattern. A disadvantage to low-pressure sodium is the monochromatic yellow light it produces, which some people find objectionable.

Important items to consider for nighttime camera lighting are illumination level, camera sensitivity, lens type, light-to-dark ratio, area of illumination in the camera field of view, and lighting position. Note: These are not simple issues to be addressed by a neophyte. Be certain that you discuss lighting issues with your local power company or lighting expert.

*Illumination level, camera sensitivity, and lens type.* Lighting levels must be high enough for the camera to produce a useable image. The light level required will depend on camera sensitivity and lens type and quality. Black-and-white cameras generally have more light sensitivity than color cameras and are recommended for most nighttime applications. A minimum illumination level of 1.5 foot-candles, as measured on a horizontal plane 1 foot off the ground, is recommended for a black-and-white camera with a sensitivity specification of 0.007 foot-candles faceplate illumination. This assumes the camera has a good-quality, F/ 1.4 fixed focal lens. A color camera or a camera with a zoom lens will require a higher light level in order to get equivalent brightness and contrast.

**Light-to-dark ratio:** A recommended maximum light-to-dark lighting ratio is 6 to 1 (as measured on a horizontal plane 1 foot off the ground). This maximum applies to the entire area of interest that the camera is viewing. It is also recommended to design the lighting for a 4-to-1 ratio to allow for some degradation over time. A 6-to-1 light-to-dark ratio will prevent areas that are so dark or so bright that a person or object would be obscured.

**Area of illumination in the camera field of view:** A minimum illumination of 70 percent of the camera field of view is recommended. A camera is an averaging device. If too little of the field of view is illuminated, the camera will average between the illuminated areas and the non-illuminated areas, resulting in blooming and loss of picture detail in the illuminated area.

**Lighting position:** The position of lighting in relation to the camera field of view is also important. As much as possible, light sources must be kept out of the camera's field of view. Lights that are illuminating a camera scene should be mounted higher than the cameras. When determining a location and field of view for a camera, extraneous light sources, such as building-mounted lighting for pedestrians that will be in the camera view, must be considered. Extraneous light sources can cause blooming and streaking in a camera, rendering portions of the field of view unusable. Distant light sources that are relatively dim are usually not a problem.

**Other lighting:** Another type of lighting is known as infrared (IR) or near infrared. The spectrum for this lighting is just below red and is not visible to the human eye. Most black-and-white cameras have sensitivity into the infrared. A black-and-white camera can be used with this type of lighting to observe areas at night without having lighting that is visible to humans. To make use of IR lighting, the camera must not have an IR cut filter. Cameras can be ordered without IR cut filters; be sure to specify no IR cut filter when ordering. Commercial IR light sources include incandescent and the light emitting diode (LED). The incandescent type typically uses a 300- to 500-watt lamp and a visible light cut filter. These are expensive to purchase (\$800–\$ 1,200) and expensive to operate and maintain (2,000 hours is a nominal life expectancy of the incandescent lamp). The LED type emits light in the IR and is also expensive to purchase (around \$1,200) but uses less power and has a much longer life expectancy. The incandescent type will provide more illumination than the LED type. With either type of IR light, more light fixtures will be required to illuminate an area than with visible lighting. While IR lighting has the advantage of not being visible to humans, it is fairly expensive.

**Alternatives to lighting:** There are two camera technologies that can see at night without the use of artificial lighting. These technologies are intensified cameras and thermal cameras, though they are probably cost-prohibitive for most schools. Intensified cameras use a photomultiplier (light intensifying) tube in front of the camera imaging device. Depending on the generation of the photomultiplier tube, these cameras can produce a picture in conditions ranging from moonlight to starlight. Disadvantages of these cameras include initial costs, maintenance costs, and lower resolution. Costs for an intensified camera can begin around \$8,000. The photomultiplier tube has a life expectancy in the range of 8,000 to 10,000 hours, requiring replacement every 1–2 years depending on the amount of use. In terms of horizontal TV lines, intensified cameras have lower resolution than a good-quality surveillance camera.

Thermal cameras are sensitive to thermal energy radiated by objects. The low-end and minimum-performance thermal cameras start around \$7,000. The high-performing thermal cameras range up to \$30,000 and require equipment for cooling the thermal imaging device. This cooling equipment can be maintenance intensive. Resolution is also lower than in general CCTV surveillance cameras.

### ***Covert cameras***

There may be times when it is suspected or known that unlawful events, including drug deals, fighting or intimidation, vandalism, or nighttime theft, are occurring on campus. With cameras in plain view, it is clear to all where not to carry out such dealings, but where incidents of concern are out of sight, it may be beneficial to temporarily install a camera hidden from view of the suspects. (Schools should make certain that they consult an attorney before utilizing hidden cameras). Cameras hidden from the view of suspects under investigation are referred to as covert cameras. In school applications, these cameras are generally hidden behind a wall or ceiling or within a common building fixture.

In some instances, it may be practical to use a normal size, readily available camera if a convenient hidden location is available, such as behind an air duct. It would be reasonable for a school district to have at least one smaller camera available for covert applications. A whole new industry has arisen in the past few years specializing in these tiny, easily hidden cameras that are available in black-and-white or color. Microphones are included with some cameras, but caution is advised in their use due to state laws regarding privacy of conversations. An amazing array of disguised cameras already installed within smoke detectors, clocks, speakers, light switches, junction boxes, neckties, caps, and so forth are available in security trade journals; it is then up to the security department to appropriately place the item where it will not be suspicious. The size of available covert cameras themselves measure about 1.25 inches square. The lenses, including pinhole lenses, come in sizes ranging from 2.5mm to 25mm. Covert kits will provide both the camera and a set of several lenses that will handle a wide range of applications, from wide-angle to telephoto. Passive infrared cameras and surface-mount cameras also are available. They can allow surveillance in some low-light environments. Voltage requirements for cameras are normally 9 or 12 volts dc and can be battery powered.

The video recorder needed to record the images captured by a covert camera must also be hidden from view. This may not be a simple matter. The smallest video recorder is much larger than the smallest camera. It requires ventilation, a somewhat clean environment, accessibility, and it makes noise. It may be necessary to install the recorder in a separate secure room or even in another building. The video signal must be transmitted from the camera to the recorder. Coaxial cable is needed for these connections. Wireless covert board cameras are available. Although their use can greatly simplify installation, their transmission ranges are limited to about 300 feet.

Covert black-and-white board cameras start at around \$150, with a resolution of about 380 lines. Color covert cameras are close to \$300, with a resolution of around 330 lines. For these operations, black-and-white cameras may be adequate or even desired. Many covert situations occur in fairly small areas, and a higher resolution black-and-white camera may be more appropriate than a lower resolution color camera. Cameras already mounted covertly within a fixture can cost between \$250 and \$500. Wireless cameras can range from \$500 to \$1,000 or more.

### ***Maintenance and expected lifespan***

After successful installation, the required regular maintenance of a fixed camera is normally to clean the outside lens. Depending on the strength of the camera's mounting and the stability of the structure it is attached to, occasional repositioning of the camera to correct the viewing angle may be required, especially for exterior applications. It is not unusual to see one or more incorrectly positioned camera scenes on the monitors of an established security communications room because regular maintenance of camera mountings has not been provided.

Housings will protect the camera lens from dust and dirt, but the glass front of the housing must be kept clean. Some super housing comes with own wiper blades and wiper fluid dispenser. The dispenser mechanism is activated remotely by an operator to keep the camera scene clear. However, this feature can add to the required regular maintenance as the dispenser must be refilled with fluid as needed.

The dome enclosures for interior ceiling-mounted cameras (usually pan-tilt-zoom cameras) are intended to reveal the presence of a camera but not its current direction or field-of-view. Dust (or mischief) can obscure the view, but otherwise, maintenance is low.

The average lifespan of a modern solid-state camera is greater than 5 years. Many camera failures occur early in a camera's life. This allows for most cameras with defects to be returned during the warranty period. Cameras do occasionally need repair so the availability of parts should be considered. This can make a good deal on an older camera system less fortuitous. If a camera unit used in a critical application must be sent away for repair, it is wise to have a backup camera available. Maintenance contracts should always address repair time and the availability of loaner units. In the absence of a maintenance contract, there are many local repair shops in most medium and large cities. Check the availability of local repair options before you purchase your system. There are several resources for camera maintenance available to customers across the country that are willing to ship their equipment; repair generally takes less than 2 weeks. Most of these resources may be located on the Web.

### ***Price Ranges***

Standard-resolution solid-state cameras can cost between \$150 and \$1,000. High-resolution cameras can range anywhere from \$900 to \$8,000. For most school applications, the standard-resolution camera is probably adequate. The less expensive cameras (nearer to \$300) need more light to accurately capture a scene. The more expensive cameras (\$1,000 or more) tend to be more sensitive, using more sophisticated electronics so that they require less light to accurately capture a scene.

### ***Going out on bid for equipment and system maintenance contracts***

While it is difficult to prevent every possible mistake when going out on bid for CCTV systems, there are a few commonsense approaches that should be incorporated in every request for quote (RFQ). The security equipment industry is no different from any other supplier - they will bid on and provide what is asked for. Even generally standard options that would seem reasonable to assume would be included should not be assumed to be part of any RFQ. If you can precisely describe what you require, the bidders will be less apt to submit bids on dissimilar systems.

Do not accept or pay for a camera system until it has been installed and is demonstrated to operate according to your specifications. Remember, the vendor doesn't like surprises any more than you do so specify your acceptance criteria very clearly in the RFQ. This includes the "quality" of installation; occasionally a contractor may try to save money by merely tacking cabling along the top of a wall instead of running the cabling within a conduit and within the ceiling. Don't assume anything.

When going out on bid, the ideal specifications for a CCTV system would describe the desired capabilities or goals of the system, not the quantities of different components. For example, if it is desired to have cameras viewing the locker bay area to discourage and identify daytime thieves; do not request "two cameras, one installed at the end of each hallway." A more profitable request could be, "The images saved to videotape and viewed on the system monitor will allow the customer to distinguish, as a measure of acceptance testing, between the geometry teacher and the school secretary standing anywhere within the locker bay area, with at least one image per camera captured and recorded per second. Quoted product and installation should be vandal proof, such that an individual, given a few minutes of uninterrupted time, would not be able to vandalize the equipment without being recorded on tape, CD or DVD and being identifiable, providing they are not wearing any type of mask." Include room dimensions and even a few photographs of the area for which the requested equipment is intended, or offer all potential bidders a tour of the area.

It is common for the prices received from such a request to be substantially higher than the school originally intended. It is efficient to include a request in the original RFQ for two different camera layouts and their associated costs. One layout would provide the exact capability requested. The second layout would be the best possible configuration within a specified dollar amount, with the expected capabilities as well as deficiencies that are expected with this layout, clearly identified by the vendor. It is to both the school's and vendor's benefit to request these two different layouts—a principal or security official armed with such information can approach the school district or school board to request the additional funding necessary to meet the goals of the security system if the less expensive system will perform substantially below the school's requirements.

Typical warranties on video cameras are 90 days, with up to a year or more for more sophisticated cameras. It is common for cameras that are defective to fail fairly quickly after installation. Be prepared for this. Assign a person to be responsible for checking regularly on the functioning of the equipment and to immediately remove failing components and return them to the manufacturer within the warranty period, or to contact the vendor and make certain that he responds in a reasonable amount of time.

If a school does desire to have a maintenance contract, either because of lack of internal manpower or because of available funding, the vendor should specify the maximum time it will take to respond to calls for help and the maximum time the customer will have to be without this equipment if a repair is required. It is possible for a school to request faster response times or even that the maintenance contractor provide loaner equipment for any down time greater than 24 or 48 hours; however, this will increase contract costs.

**Signage for use of cameras on school grounds:** Very visible and obvious signs at the entrances to a school campus and at major entrances into school buildings serve many purposes. Their value to security should not be underestimated. Signs are not overly expensive, but the price of not having one can sometimes be astronomical.

Signs that inform the public and the school occupants that certain security measures are in force can provide a frontline deterrent. Without any other knowledge, an outsider faced with the choice of vandalizing a school with security warning signs or a school with no signs or other obvious indications of self-defense will choose the latter. As described in the section of this manual on legal issues, liability can be minimized through the use of signs. A piece of information that can be important to include on a warning sign is whether cameras are not being monitored. There have been a few lawsuits in the United States that have been filed and consequently won because someone at a facility was attacked, but the victim did not try to defend himself or herself against the perpetrator. He or she was under the impression that, because a video camera was aimed directly at him or her, help would surely arrive soon. This is a common assumption. Sample wording for a school sign regarding this particular issue could be:

*WARNING: This facility employs video surveillance equipment for security purposes. This equipment may or may not be monitored at any time.*

Covert approaches to security can sometimes be open to contention, especially by someone who is caught in this way. The use of covert cameras can be extremely effective in providing evidence for prosecution. However, not all school districts or school boards will support their use. It may not be necessary to post signs regarding every security detail being incorporated on a campus. It may be quite sufficient to insert a warning regarding the use of covert cameras in the school policy document that is signed by every student and parent at the beginning of the school year and in the contracts signed by every employee. (Don't forget to include this information in contracts for outside services.)

### **Legal aspects of the use of video cameras in schools**

Laws concerning privacy issues and civil rights may vary widely, so before beginning any electronic surveillance program, be sure to check with your school attorney. However, the following generalities are fairly consistent across most of the country:

Cameras may not be used in an area where there is a "reasonable expectation of privacy." Examples of these are bathrooms, gym locker/changing areas and private offices (unless consent by the office owner is given). Examples of where cameras are generally acceptable are in front offices where students, employees, and parents come and go; hallways; parking lots; gymnasiums; cafeterias; supply rooms; and classrooms. The use of cameras in classrooms is often debated by teachers who want cameras for protection and teachers who do not. At this point in time, it is probably wise to use cameras in classrooms only when the teacher is given an option and notification that a camera is to be used.

Signage can be an important legal component in the use of video cameras in schools. As mentioned in the previous section, it is important that the presence of video cameras not lead a person to believe he or she will be rescued if attacked. Dummy cameras should not be used (which is in contrast to the “black boxes” on buses, in which cameras may or may not be located at any time). While a fake camera can create a temporary deterrent to some security incidents, the potential liability it creates due to a victim’s impression of being rescued quickly is not acceptable.

Audio recording is often considered to be of greater legal concern than video recording in most States. The recording of conversations is viewed as more of an invasion of privacy, as conversations often take place where the participants do not expect to be overheard.

## **Video recording equipment**

### **VCRs/ Time Lapse Recorders: the weak link**

The video cassette recorder (VCR) commonly used in some school surveillance systems, is the weakest link in the video system due to its mechanical nature. The more reliable but much more expensive digital recorder is discussed later. Industrial quality VCRs range in price from \$500 to \$4000. A school can plan to spend approximately \$500 to \$1,200 for a good-quality VCR appropriate for most of its applications. (This price range does not necessarily include some of the desirable features discussed later.) The inexpensive \$200 VCR is not recommended for non-home use.

Unfortunately, the most ignored maintenance task in most school security departments is the regular servicing and cleaning of VCRs. VCR heads should be cleaned after every 100 hours of use—about every 4 days of constant recording. This head cleaning can be accomplished using isopropyl alcohol and industrial swabs and takes about 10 minutes. The cleaning tapes that are available to clean VCR heads are not recommended, as they can cause excessive wear on the heads. The entire VCR unit should be serviced every 2,400 hours, or about every 3 months of constant use. This complete servicing includes replacement of bands and rubber components. If well-serviced, a typical VCR will last about 4–5 years with constant use. At least one moderately expensive (\$200–\$300) head replacement should be expected during this time.

Premium-quality tapes are recommended for the constant use experienced in most school applications. These tapes will cost about \$10 each and are available from your VCR vendor. Their expected quality lifespan is about 25 recordings. Recording over the same tape indefinitely is not recommended because this practice introduces several logistical problems. Sometimes incidents are reported several days after they occur, and the video of the incident has already been recorded over. A good recording plan includes 6 new tapes every fall and spring, labeled Monday, Tuesday, Wednesday, Thursday, Friday, and Weekend. Each morning, the appropriate tape is put into the VCR. If an incident occurs, that particular tape should be pulled and labeled as “removed,” along with the date it was most recently recorded on. A new tape labeled with that day of the week should replace the original. If faithfully done, this will probably be adequate for most schools. By replacing the tapes every spring and fall, the tape quality is not compromised.

VCRs operate at temperatures between 32°F and 104°F and need to be used indoors where relative humidity is less than 80 percent and the air is free of non-condensing moisture. Because an industrial time-lapse recorder is designed to run 24 hours a day for long periods of time, proper physical location of the unit must be considered. Recorders generate heat, and because heat is the worst enemy of the recorder (next to dirt), the recorder must be placed in a well-ventilated location. If the recorder is to be installed in an environment where there is a lot of dust or dirt in the air, provisions must be made to keep the unit clean. (A single grain of dirt in the right place can crack a video head.) If a recorder must be placed in a dirty environment, housing with a fan, vent holes, and filters should be used.

Another important consideration in setting up a VCR is locating it in a secure, protected area. VCRs are attractive targets for thieves, but even more importantly, tapes can be stolen or destroyed if there is an illegal

incident to be covered up. VCRs should usually be placed in a strong locking cabinet within a locked room. Only the school principal and one security person should have the key to this cabinet.

## **Multiplexers**

Multiplexers can be used to combine two or more individual video camera signals and send them to a single recorder. This is often referred to as timeshare multiplexing and allows up to 16 video camera signals to be recorded on a single half-inch videocassette simultaneously and played back as individual pictures or combinations of pictures upon command. A multiplexer could be either a simplex multiplexer or duplex multiplexer. The simplex multiplexer can only display a full-screen image of one selected camera or a sequence of selected cameras while recording. A duplex multiplexer can also display multi-screen images while still recording. Essentially, a multi-screen display consists of a split screen that allows for the viewing of all camera images on the system simultaneously.

Timeshare multiplexing can also be used to transmit up to 16 video camera signals from one point to a second point by a single cable or transmitter (microwave, fiber optic, infrared). Another multiplexer at the second point can be used to separate the multiple video signals back into individual video signal outputs.

A duplex multiplexer costs more than a simplex multiplexer. Generally, a duplex multiplexer is used if someone is watching or operating the system while it is recording. If it is unmanned, as in many school applications, a simplex multiplexer is more cost-effective. A true duplex system allows the user to watch multiple screens while recording without affecting the multiplexed output to the video camera recorder (VCR).

A simplex system allows for full-screen or sequenced viewing in the record mode. If multi-screens are activated during the recording, the multi-screen itself might be recorded, thereby not allowing full-screen playback. A duplex system also allows for recording and playback simultaneously if two VCRs are connected. The multiplexer should provide two monitor inputs if this feature is used so live viewing of the facility is not lost. In most applications, a simplex unit is suitable and more economical if recording can be stopped while the video is reviewed. The recorded videotape can then be retrieved in a full-screen or in a multi-screen configuration.

Most multiplexers available from established manufacturers feature camera titling for recording and a permanent time/date stamp on each frame of recorded video. Another feature is compensation for camera synchronization. Multiplexers are equipped with an alarm input for each camera. When activated, these can be used to generate an output to the VCR to place both the multiplexer and VCR into the 2-hour recording mode (real time) for a predetermined period of time.

Some multiplexers allow only images from the alarm camera to be recorded, but others allow a choice of interleaving (every other field). Onscreen programming of the multiplexer allows for simpler programming and review of settings. Programming features should display VCR tables because it is important to synchronize the multiplexer to the particular model and brand of VCR to avoid missing crucial information.

## **Time-lapse Recorders**

Time-lapse recorders have the ability to incrementally record at specific time intervals, recording a single field or frame of video information with each increment. In the 2-hour (real time) recording mode, a video recorder is recording 60 fields or 30 frames of video information each second. To determine the time interval between pictures recorded at specific speeds, the following formula can be used (based on using a T120 tape at 60 Hz): Recording speed = Seconds between frames 120.

Because the tape is slowed down in the time lapse mode, and the video heads record only specific fields of information, some actions are easily lost. If a tape recorded in real time (2-hour) was compared to a tape



recorded at a 240-hour speed, there would be lost information between them. The slower the tape speed during recording, the more information that can be lost.

There are some low-priced time-lapse recorders (approximately \$500) on the market today, but dependability and resolution may be sacrificed if an industrial-quality recorder with at least 400 lines of resolution (approximately \$1,200–\$2,700) is not specified. A high-resolution camera and monitor may be used with good results during real time viewing, but if the playback tape has been recorded with a standard time-lapse recorder with low resolution, the results may be disappointing. For best results, a high-resolution industrial-quality recorder should be used.

### **Event Recorders**

It may not be necessary to have all the features of a time-lapse recorder. Time lapse was developed to give a continuous flow of recorded information that could span long periods of time in a very small, storable format. If a school is able to interface its intrusion detection or other type of alarm system with their CCTV system (which is viewing the area where an alarm is occurring), an event recorder is capable of turning itself on to record that event almost instantaneously. Not only does this feature allow a tape to be used for very long periods of time, as no recording is being done during uneventful times, but event recorders are generally cheaper than time-lapse recorders.

### **Digital Video Recorders**

The security industry now has access to technology that allows the digital recording of full-motion video. Over the next few years this type of system will likely become even more accessible, with an increase in digital storage technology and a decrease in the overall costs associated with hardware. Digital storing and recording have many advantages over a time-lapse or event recorder. The most important advantage is that digital recorders require no human intervention, which means no maintenance and no cleaning. On the other hand, a major disadvantage is that the security industry has yet to establish standards for compressing digital information for recording (compressed digital information takes up less storage space). Hence, it is common to experience compatibility problems between alarm monitoring systems.

For school applications, a major consideration is the increased cost of digital recorders over conventional video recorders. A minimum system for digitally stored images on a hard drive is estimated to cost at least \$3,000. Without video compression hardware/software, the digital storage system is not very practical; it has been estimated that the cost for a single stored image is \$0.94 for black-and-white and \$2.81 for color. Using the compression methods available today increases the storage capacity with acceptable video quality by approximately 10 times. The additional cost of the compression system is at least \$1,500, making the cost of the complete digital recording system about \$4,500, which yields a cost per-image of \$0.047 for black-and-white and \$0.141 for color video. For comparative purposes, the cost of storing images on a typical video cassette recorder is many times less—each T120 video cassette holds 432,000 black-and-white or color images at a cost of roughly \$0.003 per image (including the cost of the VCR).

While the cost of digital storage systems has been decreasing and will continue to decrease as technology improves and the capacity of these devices increases, the cost of tape will probably be much lower than the cost of hard drives for some time to come. Consequently, the security industry will likely parallel the computer industry in storage techniques, using hard drives for short-term storage but keeping archival storage on low-cost tape systems.

**CHAPTER THREE**  
**DETECTION PRODUCTS**

## **Walk-through metal detectors for personnel**

**Do metal detectors really work?** The basic metal detectors work very well. They are considered a mature technology and can accurately detect the presence of most types of firearms and knives. However, metal detectors work very poorly if the user is not aware of their limitations before beginning a weapon detection program and is not prepared for the amount of trained and motivated manpower required to operate these devices successfully.

A metal detection device in school security applications is used primarily to locate undesirable objects that are hidden on a person's body. When a questionable item or material is detected by the device, the detector produces an alarm signal. This signal can be audible, visible (lights), or both. Unfortunately, a metal detector alone cannot distinguish between a gun and a large metal belt buckle. This shortcoming is what makes weapon detection programs impractical for many schools. Trained employees are needed to make these determinations.

Metal detectors are usually not effective when used on purses, book bags, briefcases, or suitcases. There are usually a large number of different objects or materials located in or as part of the composition of these carried items that would cause an alarm.

If you ask the average person what a metal detector does and what property to which it is most sensitive, the answer to the first question would probably be that it is a device that detects only metal. The answer to the second question likely would be that a metal detector is more likely to detect metal objects with heavier mass. Both answers are incorrect.

A metal detector actually detects any conductive material—anything that will conduct an electrical current. The typical pulsed-field portal metal detectors generate electromagnetic pulses that produce very small electrical currents in conductive metal objects within the portal archway which, in turn, generate their own magnetic field. The receiver portion of a portal metal detector can detect this rapidly decaying magnetic field during the time between the transmitted pulses. This type of weapon detection device is “active” in that it generates a magnetic field that actively looks for suspicious materials or objects. A magnetometer, a passive device, was much more in use 20 years ago in the detection of weapons. The magnetometer depends on the Earth's magnetic field. It looks for a distortion caused by the presence of ferromagnetic (attracted to a magnet) material.

Counter to intuition, the mass of a particular object is not significant in metal detection. The size, shape, electrical conductivity and magnetic properties are the important properties. For example, when a long thin wire is taken through a portal (walk-through) metal detector, and the wire is in any geometry except one in which the two ends (or any two points on the wire) are touching, it will rarely be detected. However, shape this same wire into a closed circle and the metal detector will most likely go off, even though the mass of the wire has not changed.

Delving even deeper into metal detector sensitivity, consider the orientation of an object. Take the same closed-loop wire described in the previous paragraph. Lay this loop on its side so that it is parallel to the ground. In this configuration, the portal metal detector is less likely to see it, but if the wire loop is upright and parallel to the side panels of the metal detector, the detector will be much more likely to go off in this orientation.

Some people fear the use of a metal detector on themselves because of the possible side effects of being subjected to the magnetic field. This fear is unfounded; metal detectors emit an extremely weak magnetic field, weak enough to be of no concern even to heart patients with pacemaker-type devices. Indeed, the use of an electric hair dryer subjects the user to a much stronger field than would be received by a metal detection device.

Another widely held belief about metal detectors is that they are a straightforward technology, where the equipment does all the work. This is not true at all. The average first-time consumer will undoubtedly expect a metal detector to be much smarter and more helpful than it can possibly be. A metal detector is only as good as the operator overseeing its use.

The misconception exists in many facilities that someone known by the operator, such as a fellow employee or a security person, should be allowed to circumvent the system. It must be clearly established that in order to ensure the integrity of any routine metal detection program, everyone must be subjected to the program requirements, including students, parents, teachers, custodial and maintenance staff, security personnel (except for sworn police officers who are required to carry a weapon), school administrators, and visitors. To require less would be counterproductive and prejudicial. Signage can be of great help: a sign at the school entrance explaining the importance of the detectors in maintaining a safe and comfortable learning environment provides policy notification. If a more aggressive approach is needed for a particular community, entry signs could spell out a particular school or district policy that requires the screening of all who enter the school, with access denied to those who refuse.

### **Space requirements and layout**

The portal metal detector, also called a walk-through detector, is a stand-alone structure that resembles a deep door frame. The typical walk-through detector will take up a space on the floor about 3 feet across and 2 feet deep. This does not mean that if you have 3 feet by 2 feet space at the entrance to your facility you necessarily have space for using a walk-through detector. The typical height of most portal detectors is around 7 feet. Weight of a unit can vary from around 60 pounds to as much as 150 pounds; however, the awkward shape of most portals prohibits their being easily moved by one person. Portals are generally freestanding and are rarely attached to the floor or surrounding structures. Power requirements are for one plug to a typical 110-volt wall outlet.

The first space factor to take into consideration is where people who are waiting to walk through the portal (scannees) will stand. Ideally, there would be no wait for use of the portal, but this is probably unrealistic in a school environment where the entire population of students will be arriving over a very short period of time. Each school has to determine how many scannees will arrive and at what rate. Most detection programs will need to operate indoors or at least under some type of shelter, and most schools are going to want to provide a comfortable environment for those waiting. This usually means that there must be enough shelter for the queue of scannees that might build up at any one time and that they should not be overly crowded. There should also be some way of clearly forming a line for scannees to stand in if they will be arriving at a much greater rate than can be processed. Eliminating the opportunity for cutting in line would clearly be important in a school to reduce possible fights.

To avoid sending conflicting signals to the detector, the scannee waiting in line to use the portal next should be kept back 3 feet from the current user walking through the portal. Operators of the equipment and scannees who have already walked through also need to be at least 3 feet from the portal in all directions. (Contrary to a scene in a popular movie of several years ago, a gun thrown along the outside of a metal detector by the scannee before entering the portal and retrieved on the other side after the scannee walked through would cause an alarm.) Likewise, if more than one portal metal detector is being used, each needs to be at least 10 feet from the others unless they have been synchronized.

Without very special instructions and limitations for the scannee population, it would be most difficult to conduct a metal detection scanning program with only the use of portals. Hand-held scanners are usually required for use on scannees who have triggered an alarm walking through the portal but who fail to be able to immediately determine what object on (or in) the person caused the alarm. Also, it is highly recommended that any routine metal detection program incorporate the use of x-ray equipment for book bags and purses because of the ease with which a contraband item or material could be hidden within carried baggage. (See the sections in this chapter on handheld metal detectors and x-ray equipment for baggage.) This equipment mandates additional space.

Space for the scannee to follow procedures is also required. A person about to walk through the portal needs room to place his or her carried items on the x-ray machine, room to put his or her pocket items (coins, keys, heavy belt buckles) in a special pass-through container, space to pick up these items, and space to turnaround to walk through the portal a second time if necessary.

It is very important that there be neither space nor opportunity for particular members of the population, including employees, to walk around the detection system. Very definitive boundaries must be established to prevent circumvention of the system and prevent pass back of contraband, where such prohibited items are handed from outside the screening area to those who have already successfully cleared the scanning process.

In designing the layout of the metal detection system, the composition of surrounding walls, furniture, nearby electromagnetic equipment (such as an elevator), nearby plumbing in the walls, and even metal trash cans must be taken into account. The optimal effectiveness of a portal metal detector can be easily degraded by a poor location, a casually placed metal stool, or the nearby use of electromagnetic devices. See the section about sources of interference elsewhere in this chapter. In schools, the metal detection equipment and personnel will generally be located directly within the front or main student entrance. Unfortunately, the design of most schools does not lend itself to a comfortable staging area for this process. There is usually not nearly enough interior or covered space to allow for all the students waiting, entering the system. This may mandate that the metal detection staging area be located further within the facility, which may place administrative offices outside the cleared area. Conscious decisions must be made and potential risks must be realized when designing the weapon detection program.

A greater problem is often that the layout of schools will not allow for the limiting of only one or, at most two, entry points. Few schools can afford to have multiple entry setups with complete metal detection programs. The cost of the equipment would be quite high, but not nearly as prohibitive as the manpower to run these multiple systems.

### **Throughput**

A well-trained and motivated operator should generally be able to process between 15 and 25 people per minute through a portal detector. This does not include investigation of alarms, nor does it take into consideration intentional or unintentional delays that might be expected in a student population.

Assuming that scanning personnel are well-trained, a school's throughput is going to be driven by three things: (1) the number of devices, (2) the rate at which students arrive, and (3) the motivation of the students to cooperate and move through the system quickly and the ability of the school staff to make certain that scannees move along quickly. The breakdown of equipment or the arrival of visitors who are not familiar with the scanning routine will also cause a definite slowdown. The impact of this must also be considered by the school administration but is not taken into account here. The need for backup equipment must be considered by each facility, whether the equipment is borrowed from the vendor or a pool of spare equipment is shared within a district.

Keep in mind that any population that is aware that it has to regularly go through the scanning process will soon compensate and adjust their routine. These adjustments will generally be that (1) the population will attempt to take fewer prohibited items with them into the facility, (2) scannees will learn which otherwise acceptable items in their possession will still cause an alarm and will tend to shy away from these items (except maybe in the case of students who wish to create a hassle and who are undaunted by any consequences for doing so), and (3) the population will allow for the additional few minutes in their schedule, perhaps even going so far as to come early enough to miss the main rush.

Travelers flying out of busy airports know to allow for a few minute delays at the metal detection scanners and will not cut their arrival time so close that they miss their flight. Students will do likewise, whether they need to show ID cards at the front gate go through a metal detection system or meet with their friends before class. However, unreasonably long waits of 15 minutes or more could result in staff, students, and parents

alike reevaluating the need for a metal detector program. No one wants to add significantly to their workday, especially if they are not compensated for it. Employee organizations may bargain for extra pay for this additional at-school time. The average number of students waiting at each 5-minute interval before school to enter the weapon detection system for a school population of 1,000 and 2,000, is 25 and 50, respectively. For these calculations, it was assumed that metal detection equipment is in good working condition and optimally laid out, operators are motivated and comfortable in their tasks, and students move smoothly through the process. The arrival rate resembles a school morning where the bulk of students arrive within a 10- or 15-minute window, perhaps resembling a school whose students rely primarily on buses for transportation. (Whether or not the assumed arrival rate is truly typical of student arrival times is unknown. It is used here is for discussion purposes only.) The overall throughput is gauged in terms of the number of students who will be waiting to enter the metal detection process at any particular time. The assumption is made that the portal metal detector will be the bottleneck of the scanning process and that other supporting components of the detection program will be able to perform their functions in an equal or lesser amount of time (although this may not necessarily be true at a particular school, depending on its setup). It is also assumed that the process will be set up such that students who fail the initial portal screening will be immediately funneled to an alternative screening point and will not have to reenter or further delay those at the main entry portal.

For students prepared to clear the portal who have minimized alarm-causing items and materials in their possession, the actual processing time through a metal detection program should be less than 10 seconds. For students who are not prepared, the processing time may add an additional 3–5 minutes or more for scanning the body with hand-held metal detectors and/or manual bag searches. This does not include the additional delay of waiting to be scanned.

After carefully calculating the necessary metal detection equipment, space, and personnel, and making adjustments for individual school characteristics, the administration may realize that there simply aren't enough resources available to handle its students in an acceptable manner. Some schools have overcome these limitations by staggering the school day start times for students, thereby spreading out the school's limited metal detection resources. Unfortunately, schools that rely heavily on bus service may not be able to utilize this solution.

### ***Hardware costs***

Portal metal detectors vary widely in price. Portals on the market range from as little as \$1,000 up to as much as \$30,000. The moderately-priced models around \$4,000 to \$5,000 probably offer the features and reliabilities required for a school metal detection program. Models closer to \$1,000 are not recommended due to lack of sensitivity of these devices. Models in the higher price ranges generally offer enhanced capabilities that would not be necessary or warranted in a school environment.

To make any metal detection program effective, school access during the rest of the school day, during off-hours, and during special activities needs to be tightly controlled. A motivated student can defeat a lax system. If there is a comprehensive metal detection program at the front entrance to the school, but the back entrance through the cafeteria is unguarded, the funding and efforts put into a well-meaning program can be wasted. A successful metal detection program cannot be poorly funded or run by an administration that is reticent to make major changes to school policies and procedures.

### **Hand-held detection**

#### **The name of the game: Policies and procedures**

Battery-operated, hand-held metal detection devices are a very viable technology for use by schools, and most detectors on the market work quite well. By moving the wand of a hand-held metal detector around and close to a scannees body, the operator can fairly accurately locate sources of metal (or more accurately, sources of conductive materials) that may be on, or even in, a person's body. When a suspect area is located, the hand-held device will generally give off an annoying squeal. These devices do not have the ability to

discriminate between an actual weapon and some piece of benign metal. The responsibility of the operator of the device is to judge whether the squeal he or she heard is truly suspect, then to investigate and determine the cause of it. A very common use of hand-held metal detectors is in airports, where these devices allow the security staffs to more accurately locate the source of an alarm on a scannee's body, after a scannee has already walked through a portal system and caused an alarm.

Although most hand-held metal detection devices on the market work well, the hand-held metal detector is only as good as the operator using it. Some vendors and users of hand-held metal detectors say that there are only three things that need to be considered for their successful use: procedures, procedures, and procedures. A disinterested or unmotivated operator can negate much of the benefit that could be derived from a school's metal detection program. While it is not difficult to learn to use a hand-held metal detector correctly, school administrators should not underestimate the value of annual training for their operators, as well as training for staff that may be called upon to serve as backup or supplemental operators. A complete training course, including practice time, should take no more than an hour. However, on-the-job practice is definitely an important part in allowing the school to achieve the throughput that will be required to process students quickly.

Policies and logistics for use are also very important. Though hand-held metal detectors are affordable, it would be unusual for a school of any size to screen all students and employees each morning using only hand-held detectors. Manpower would be far and away the major cost of such an endeavor. Using a throughput rate of about two students per minute, a school would need one operator for a full hour for every 120 students. This assumes the students' arrival rate is evenly spread across 1 hour, which is not very likely.

If a school is attempting to do a complete screening of students each morning, the hand-held metal detector will more likely be used as a supplement to portal metal detectors. As in airports procedures, the handheld detectors allow the security staffs to more accurately locate the source of an alarm on a student's body, after a student has already walked through a portal system and caused an alarm.

Most schools that desire to establish some type of weapon detection effort (but less than a full-scale, every-morning, every-person effort) will set up a policy to allow random spot checks on students or complete student population scanning as deemed necessary. It is very difficult to do truly random checks with any hope of locating weapons. There is almost always a small but distinct group of kids that a school is most concerned about possibly carrying a weapon. These high-risk students are going to object if you search them more than once, and they would quickly compensate for this anyway, by forcing another student to carry their weapon onto the campus for them. One of the more successful approaches being used is for a school administration to choose an entire classroom at a time and scan every person (including the teacher) in the room.

Complete student population scanning with only the use of hand-held detectors can be undertaken when a school feels that major weapon issues are evolving suddenly and quickly, i.e., a member of the school. Staff has received information from a reliable source. The school administration and staff need to realize the great amount of time this will take and be prepared to handle the discipline of the crowd of waiting students.

One approach that may help some schools is to establish a policy that allows the school to do a weapon detection scan of any student who arrives at school early or late in the morning. This may provide the school with a lot of leverage. There could be some excellent deterrence created if students knew they would definitely be scanned when they are early or running late. It would also be beneficial for information regarding the potential use of metal detectors at school events to be printed on all tickets for games, dances, and so forth.

A school should seriously consider having both a male and a female operator of hand-held detectors in order to perform scans on students of both genders.

## **Space requirements**

The use of hand-held metal detectors requires only slightly more space than that already occupied by the operator and the scannee. Unlike portal metal detectors, hand-held metal detectors are not nearly so sensitive to their surroundings. Their sensitive zone is usually within just a few inches of the device's paddle. Metal walls, elevators, fluorescent lights, and plumbing that can affect portals do not usually have any affect on hand-held devices. The school must provide enough space for the students who are waiting to be scanned and about a 6-foot by 6-foot area for the actual scanning process. It is also necessary to have a table or other stable structure for students to place their purses and book bags on and for them to lean on when they lift their shoes to be scanned.

It is not recommended that this scanning process take place in a private room or area. To avoid possible misconduct, accusations of misconduct, or a confrontation with a student who does end up actually having a weapon, all of the weapon detection program functions should be performed in view of everybody else. The exception is the unusual circumstance wherein a person is suspected of hiding some type of contraband in a private area of their body.

## **Throughput**

In an environment where scannees are unfamiliar with the routine of hand-held metal detector use, such as at a courthouse, accurately scanning an individual may take as much as a couple of minutes to do well, especially when there are multiple alarm sources on one person, i.e., belt buckle, pocket knife, and steel shanks in boots. However, in a school environment, after the program has become routine, and where the students are generally cooperative and anxious to get through the metal detection system quickly, it should take no more than about 30 seconds to scan an individual with a hand-held detector. Assuming there are no difficult or ambivalent students, most schools can plan to hand scan two students per minute per operator.

A good routine for any school weapon detection program involves training the student, staff, and parent populations. If the program requirements are repeated in presentations, in classrooms, and in writing, it will take much less time to settle into a routine. Instructional posters located at the scanning equipment should include diagrams of how a scannee should stand. For a complete, full-scale metal detection program to be held every morning for every member of the school, about 1–2 weeks will be needed for students to acclimate themselves by coming a few minutes earlier and wearing clothing and accessories that are less suspect. The first week of any metal-detection program will be chaotic.

## **Hardware costs and manpower costs**

Most hand-held metal detectors on the market range from about \$20 to \$350. Schools should plan to spend between \$150 and \$200 for detectors that have desirable features, including a long detection paddle (to reduce the amount of passes necessary across a person's body), a warning light or beep when the batteries begin to run low, and an audible feedback alarm that squeals louder or changes pitch for larger suspicious items and softer for less suspicious items (such as a zipper). Even the least expensive detectors will work, but more time may be required to perform a complete scan, and the procedures for the scan may be more intrusive. These smaller detectors are convenient if a school administrator or security person wishes to carry a smaller detector on their belt at all times.

Hand-held metal detectors run on either a 9-volt battery or on a rechargeable NiCad battery. A new or freshly recharged battery will last for approximately 1 hour of constant scanning. The rechargeable units may require that the battery be recharged by itself. Other hand-held detectors have a jack or plug built into them so it is unnecessary to remove the battery to recharge. (It is suggested that for hand-held detectors that are used very infrequently, such as once a month, batteries should be removed when the unit is not in use.) A staff member should be assigned the responsibility for recharging batteries each night and/or making certain that new batteries are always available.



Obviously, manpower costs drive the use of handheld metal detectors. As mentioned in the section on throughput, a trained operator can scan approximately two people per minute. For each operator and all backup operators, a thorough training course along with some practice time should take no more than an hour at the beginning of each school year. A school should not forget to formally train security personnel who are hired after the start of the school year. (Some metal detector vendors provide an instructional videotape that can be useful, but the tape should not be used as the only source of initial training and practice.)

**CHAPTER FOUR**

**ENTRY CONTROL TECHNOLOGIES**

Many school administrators contend that the majority of the security problems and incidents at their schools are the result of an unauthorized person being on campus (albeit the vast majority of these unauthorized persons are in some way related to the school or to students at the school). These trespassers can include a school's own suspended or expelled students, students from rival schools, irate parents seeking revenge against a student or employee, gang members, or even drug dealers. It is logical, then, that if a school were able to carefully control exactly who was able to enter the campus or school buildings, security incidents would drop significantly. This is easier said than done.

Schools can often prevent or discourage the casual intruder. Some of the less technical, though often quite effective, approaches to deterring unauthorized entry are:

- Posted signs warning that unauthorized trespassers are subject to arrest.
- Signs that inform visitors that all vehicles brought onto campus are subject to search by the school.
- A guard who is checking identifications at the main entrance gate to the campus.
- Vehicle parking stickers so that any vehicle found parked on campus without a sticker, other than in the monitored visitor lot, is subject to being ticketed and towed.
- Uniforms for students, which make outsiders very identifiable.
- A school policy of no hats; no droopy pants; no t-shirts with alcohol, drug, violence, or gang affiliation messages; or no exposed tattoos, which again can help make outsiders identifiable.
- Greeters at all open entrances to school (these can be parent volunteers).
- Minimal number of entrances to the campus and to the school; superfluous exterior doors should be locked to prevent entry from the outside and labeled inside: "For emergency exit only—alarm will sound."
- A policy that anyone walking around campus during class time will be challenged for a pass and/or student ID and is subject to being searched or even scanned by a metal detector to be checked for weapons and/or drugs.
- The main student parking lot (which does not include parking for work-study students) closed off and locked during the day. Make entry to school during the school day possible only through the front office.
- Fencing around campus that will discourage the casual intruder and better define school property.
- A policy that, when a student is expelled or suspended, his or her student ID is confiscated and (for a larger school) his or her picture is made available to the security staff.

### **Limiting entry/exit points**

Most Idaho school buildings in use today were originally designed to foster learning, mimicking universities to some extent. Often, their layouts provided many secluded niches to allow students privacy in which to study; separate buildings to house the various disciplines; multiple entrances and exits to maximize fire safety and emphasize freedom; and spread-out campuses to prevent congestion and to be open to the community. Fences became passé, perhaps for appearance but more likely to cut expenses. Some schools even have public streets running through the campus. These designs were very appropriate and greatly enjoyed 30–40 years ago. Entry control in these facilities has been limited in the past to the coincidence of an adult noticing an outsider on campus and challenging that outsider. For current security needs, controlling the access of students, employees, and visitors has become paramount.

Without major remodeling for some schools, the manpower required to accomplish access control could be enormous, both for entry into buildings and onto the campus itself. (One fairly new high school in Meridian consists of 1 large building but has more than 20 exterior doors.) Technologies such as card swipes or keypads can greatly reduce this manpower requirement, but not without significant expense. To best control a school building and/or campus, the number of entryways into the building or onto the campus must be severely limited. Just as with any high-security facility, restricting normal entrance to only one or two locations can greatly reduce the number of security personnel or security devices that must be supported. But limiting entry points can be very difficult for some schools, due to building layout, required emergency egress, property boundaries, the surrounding neighborhood, and adjacent streets.

Some urban schools have no campus per se; their buildings sit directly on streets on one or more sides. This can somewhat reduce the entry control problem but has some inherent problems of its own. For those schools with campuses, fencing is usually important to control entry onto the school grounds. It is important that schools and communities recognize that enclosing a campus with fencing is more to keep outsiders out than to keep insiders in, although its presence does tend to reduce truancy during the school day. Controlling campus entry requires fencing or other physical barriers.

Fencing does not have to be unattractive. Razor tape or barbed wire is rarely appropriate for a school setting but may sometimes be necessary due to vandalism or theft at a school. If adequate funding is available, wrought iron fencing can enhance the appearance of some campuses, while providing a very difficult barrier to climb over. Less expensive but still providing an excellent barrier is an 8-foot chain link fence with small mesh (1-inch to 1 1/2-inch). Unlike a typical 6-foot chain link fence, it is difficult to pull up on an 8-foot high fence and a smaller mesh will not allow toe-holds. This more desirable 8-foot fencing material is usually about twice the cost per running foot as the cost of standard 6-foot fencing material, but it is probably worth the extra cost, depending on the particular school's risks.

A robust fence defines property boundaries and forces a perpetrator to consciously trespass rather than allowing idle wandering onto a campus that has no fencing. The goal of fencing is to deter the casual or unmotivated trespasser. No fence can keep out someone determined to enter the campus who comes prepared or who is very motivated (i.e., brings a ladder or wire clippers, smashes through the fence with a vehicle). Fencing may be less important for a school that is located in a somewhat remote location. If the majority of students, faculty, and visitors must necessarily get to a particular school on buses or in cars, then the act of restricting vehicle entry to one or two driveways and posting a guard at these locations to validate all vehicle occupants may be adequate without the enclosure of fencing.

For campuses where entry into the building(s) is controlled or restricted and students do not congregate outside during the day, again, fencing may be less useful.

### **Entry-control approaches**

Once entrances to a facility are limited in number, the process of allowing or denying access is generally accomplished through one of four approaches. The first and most common approach is manpower intensive, and the remaining three employ technology devices. The level of actual security achieved is generally believed to be from 1 to 4 lowest securities to highest security, but this is subject to many other variables. These four approaches are:

- A security guard controls entry; ID cards or other means of identification may be checked (WHO lets you in?)
- A special ID card/badge with automatic readers. (What you HAVE)
- A PIN number for entering on a keypad (What you KNOW)
- A biometric device for feature recognition. (Who you ARE)

**WHO lets you in:** A security person (or a person assigned to this duty) is located at some particular entry point, either at the vehicle entrance onto campus or at the main entry doors into the building. This security person establishes that the person wishing to enter is a valid student, employee, or visitor. In smaller schools, this can often be accomplished with no more than the recognition of the person by the security person. In larger schools, this validation can be accomplished through issued ID cards (usually with photos), badges, vehicle stickers, or mandatory school uniforms. Although this is not considered a high-security approach for the reasons listed below, it can be one of the most expensive approaches for most schools.

- **Strengths:** A security person can do more than simply check an ID card. He or she may also notice if something appears amiss, such as if a student is drunk or acting strangely. A security person can also prevent two or more students from entering using one ID card.
- **Weaknesses:** A security person in this task can become bored and may become careless or move to a different job. A security person's attention can be diverted. A dishonest security person could allow unauthorized individuals to enter. Using a person for entry control is an ongoing expense for the school. A simple picture ID card can be stolen and used by someone else; experience has shown that security personnel can sometimes fail to identify persons who have an ID card with someone else's picture.
- **Costs:** Depending on the part of the country, each security guard will cost between \$8,000 and \$30,000 per year, plus training, uniforms, and so forth. (This does not apply to the costs of an actual law enforcement officer.) One guard can be expected to handle roughly 250–350 cars per hour, providing that vehicle occupants are prepared to show ID immediately.
- Every member of a school's security organization must have a thorough background check before being hired, with references and previous employers called. If possible, periodically require drug testing on a random basis.

**What you HAVE:** In this approach, an ID card or badge is specially encoded to be recognized by a card reader. Validation of the card can be designed to electronically open a door lock, allow a turnstile to operate, or lift a mechanical arm that extends across a vehicle driveway. Viable card technologies for schools include bar codes or magnetic strips for card-swipe readers (such as those used for most credit cards) or passive or active radio frequency (RF) cards for proximity readers, which can validate a card several inches to several feet away (depending on the cost of the system). Card-swipe readers are probably more subject to vandalism as their read heads are fairly delicate. Proximity readers can be protected with a solid piece of Plexi-glass because actual contact of the card is not required. A proximity card reader might be an ideal entry control system for a teacher's parking lot, or for a computer lab. The newer smart cards are probably overkill for an entry control system.

- **Strengths:** No manpower is involved. These are mature technologies. Validation of a card can be turned off if the card is lost or stolen. When used in conjunction with a floor-to-ceiling turnstile, an authorized person cannot bring in unauthorized persons. It is also possible to automatically update an attendance database when an ID card is read. These cards are generally tamperproof, and some have features that make them very difficult to counterfeit.
- **Weaknesses:** For an electronic lock or vehicle barrier, there is no way to ascertain that only a single authorized person is entering. Cards can be lent out. Cards can be used by others until the card is turned off by the school administration. Card-swipe readers can be subject to vandalism if in a vulnerable location. Card readers require a certain level of overhead to maintain, and regular updating of their databases is mandatory.
- **Costs:** Prices for the equipment to produce high-quality, tamperproof ID cards, with software to develop attractive customized designs, have come down greatly in just the past few years. A sophisticated printer that embeds the ink into the card cost as much as \$25,000 just 4 years ago. Today, an entire system (a printer, a digital camera, and the software to operate them) that is more than adequate for most school's needs can be purchased for \$6,000–\$8,000. While every product is different, and there are many features that can be added that raise the price considerably, the supplies (inks, card blanks, and so forth) that a school must continually purchase to create cards readable by a card-swipe reader will cost the school about \$3 per card. Supplies for cards readable by a proximity reader will run between \$3 and \$10 per card, depending on the capabilities of the system. Card-swipe readers and proximity readers cost between \$150 and \$300 per reader. The electronics, field panel, and computer system necessary to support a modest number of readers (typically, eight or fewer) will cost around \$2,000–\$3,000. Installation is usually a job most appropriate for an electrician.

**What you KNOW.** A personal identification number (PIN) or special code is entered on a keypad. This is usually used in conjunction with an ID card and card reader. Alone, a PIN used on a keypad could be easily compromised by an onlooker; if used in conjunction with a card reader, the level of security is substantially higher. Sophistication of keypads runs from very simple entry devices to unique scramble keypads that effectively allow only the user to view the numbers and that scramble the numbers differently for each use.

- **Strengths:** The PIN and ID card can be turned off when no longer appropriate. A stolen ID card is not enough for a trespasser to use for entry. It is also possible to automatically update an attendance database when an ID card is read and the PIN entered.
- **Weaknesses:** More administrative effort is required to maintain a card system and keypad system. Except when used with a floor-to-ceiling turnstile, it is possible for an authorized person to allow unauthorized persons entry. Users can forget their PINs. Users can lend out their PINs and cards. Keypads are vulnerable to mechanical malfunction as well as vandalism.
- **Costs:** Simple stand-alone keypads, hooked directly to an electric door latch, lock, or strike, may cost less than \$200 for all the necessary hardware. However, installation may be difficult on an existing door. More sophisticated keypad systems that may be part of a network of keypads can cost from \$1,200 to several thousand dollars.
- An ideal application for a keypad system is for a relatively small population size that does not change often. (For example, the chemistry storage room that only the chemistry teachers have a code to enter.) For these applications, where the keypad is not subjected to abuse or a harsh environment, a keypad system can go for many years without any additional maintenance or adjustment.

**Who you ARE:** An electronic device verifies the identity of a person through the use of a personal attribute, such as hand or finger shape, fingerprint, voiceprint, signature dynamics, retinal pattern, or iris pattern. These devices, known as biometric identifiers, can be very accurate. The chances of such devices mistakenly allowing an unauthorized person into a facility is usually much lower than the chances of a guard inaccurately matching faces to picture badges. Biometrics is commonly used in high-security applications where unauthorized access into a facility is unacceptable.

- **Strengths:** This form of identification cannot be lent to other people. A particular person's identification can be deleted from the database when no longer appropriate. There is nothing for a user to forget to bring with him or her. Hand or finger geometry appear to be viable, affordable, and user friendly biometric devices for medium- or low-security applications. Retina or iris pattern scanners are probably the most accurate of all biometric devices, and are most appropriate for high-security facilities. Voice recognition systems have improved significantly over the past few years but still have some weaknesses to overcome before their use is widespread.
- **Weaknesses:** Not all biometric devices are user-friendly. Some devices are very difficult for certain individuals to use. Except when used with a floor-to-ceiling turnstile, it is possible for an authorized person to let in unauthorized persons. Some of these technologies are not completely mature, in that their occasional tendency to falsely reject an authorized person can be unacceptable in a school environment. The devices are subject to damage from vandalism. It usually takes longer to use a biometric device than a card reader or keypad.
- **Costs:** These technologies continue to improve and new biometric devices are always being brought to market. Prices for most of these devices have stabilized over the past 5 years. A stand-alone biometric unit can run between \$1,200 and \$5,000. A system that oversees and monitors biometric units at several doors can cost between \$10,000 and \$50,000.

*Working with vendors:* Identification cards that are readable by an electronic device are probably the more viable technology for schools to consider for entry control. Dozens of different manufacturers are offering hundreds of devices that produce a wide variety of card styles and features. Visiting one of the security trade shows, such as the American Society of Industrial Security (ASIS) conference held each year, will familiarize an individual with most of the products available on the market. Some good questions to ask the vendor are:

- What is the cost of the basic printer, basic digital camera, and basic software? What additional features are available for each of these, how much are they, and what do these upgrades provide?
- What kind of computer will be required to run the system and with what memory and storage capabilities? What is the general speed of data input and card production that can be expected? What can be done (e.g., upgraded components) to speed this up? (An acceptable system may take between 1 and 2 minutes to produce one ID card.)
- Does the printer create both sides of the cards at once, or does the card have to be manually flipped?
- Will the vendor come and install the system and get it working initially?
- Will the vendor program the software initially for the first card design?
- What is the bulk cost of all of the supplies that will be needed? Is it reasonable to buy enough supplies for the next several years, or do some of the materials have a limited shelf life? How long are these particular supplies expected to be available?
- What maintenance is required on the printer and how often (i.e., after how many cards?)
- How long does it take to turn the system on before it is prepared to accept data for the first card?
- Is there any limit on the number of cards that can queue up waiting for the printer at any one time?
- What additional security options are available for the cards? (For example, some vendors offer hologram overlays, which may add \$0.25 to the price of each card.)
- What are the names and phone numbers of schools in your State that are already using this device? How long have they had their systems?
- Did the other schools using this system find it difficult to use the system? Is training simple? Have they had any equipment breakdowns yet? Did any of the supplies not produce the number of cards they said it would? How many additional blank cards should be purchased for errors, redo, and so forth?
- How much space is necessary to set up the equipment and allow enough room for operators and waiting students?
- What happens if the system breaks in the middle of the registration of students?

## **CHAPTER FIVE**

# **DURESS ALARM DEVICES AND THEIR ROLE IN CRISIS MANAGEMENT**



It would be very unusual for a school to never experience a crisis situation. A crisis can be any incident whereby the health or well-being of one or more students or one or more employees is in imminent danger, or part or all of the school facility will potentially be destroyed or made unavailable. A list of crises could include:

- A threatening or drunk student or employee.
- A trespasser on campus.
- A fight.
- The breakout of a contagious disease.
- An irate and threatening parent on campus.
- Sudden unavailability of a teacher or a bus driver.
- A weapon known to be on campus.
- Massive vandalism.
- A utility outage (no water, electricity, heating, cooling, or telephone service).
- Bad weather (weather too bad to allow students to return home via normal methods or at normal times).
- A vehicular accident with injuries, either in or near the school parking lot or during a school-sponsored event.
- An extremely ill student or employee.
- A gas main leak or toxic spill on or near campus.
- A bomb threat.
- A gang confrontation on or near school property.
- A suicide.
- A hostage situation.
- A shooting, stabbing, murder, or rape.
- A bomb detonation inside the school facility or adjacent to school facilities (a car bomb).
- A local or National emergency that sends community residents to seek temporary shelter at the school.
- For a school, a crisis that requires immediate response can be as harmless (but inconvenient) as the lack of a key to open the gym for an evening sporting event.

Unfortunately, recent tragedies in the United States have demonstrated the need for schools to be prepared to respond to emergencies as serious as shootings or bombs. How a school responds to this wide range of incidents is in itself an entire discipline—that of crisis management and planning. Every school needs a well-thought-out, annually updated crisis plan, with regular training for all those who might be involved. Not all schools have a plan, and many plans in existence were issued by the school district such that, by virtue of their generic nature, they may be inadequate for a true emergency. This plan needs to make assignments of who is in charge during different types of emergencies; who is the alternate in charge; who is called first, by whom, from where, and using what; whether students are relocated and how; how students are provided food, water, or shelter in the interim; what type of statement is made to the press and by whom; and who is in charge when emergency teams (fire, police, and so forth) arrive on the scene. These are only a few of the specifications called for. In the best of all possible situations, a predetermined team of school employees will immediately muster upon occurrence of a serious situation. Team members would know who to look to for decisions and then proceed automatically in their roles for the particular plan chosen to be implemented.

For the sake of this discussion, it will be assumed that a school has a current crisis plan in place. The issue that will be of concern here is how an employee (or student) can notify security, school personnel, and/or local emergency services that a crisis is occurring or is imminent. Types of communication that may be viable are yelling or screaming, sending someone else for help, using the public address (PA) system, using a telephone, or calling on a two-way radio. (Two-way radios will be a selected technology topic in a subsequent manual.)

Now consider that the person who needs to summon help is in a situation where these options are not viable. This situation may be constrained by the need for extreme urgency or discretion (because of an intimidating

situation) or because of the vulnerable location of the person summoning help. The provision that allows a person to summon help under one or more of these constraints is defined as a “duress alarm.”

Modern duress alarms are generally electronic devices that vary widely in capabilities and price. There are three general overlapping categories of duress alarms that can send one or more levels of distress signals to a particular location:

- A panic-button alarm—a pushbutton mounted in a fixed location.
- An identification alarm—a portable device that identifies the owner of the device.
- An identification/location alarm—a portable device that identifies, locates, and tracks the person who activated the duress alarm.

(One additional category could possibly be the cellular telephone. While this approach is neither as discrete nor as automatic as the other three categories of alarm devices, a cellular telephone is highly recommended equipment for every principal and the primary security person. Land lines for telephone service are occasionally unavailable, whether due to inclement weather, accidents, or through malicious actions.) The panic button is by far the most common type of duress alarm presently found in schools. The simplest application would be a strategically located button that, when initiated, would engage a dedicated phone line. A prerecorded message specifying the school, its location, and the urgency is sent to several locations, such as the police department, the district security office, and so forth. Such a system could be pulled together for a few hundred dollars by the local handyman, plus the ongoing cost of the phone line.

Commercially available duress panic button systems provide a pushbutton mounted on classroom walls or under teachers' desks. In a duress situation, a teacher or other employee depresses the panic button, which transmits a signal, via wiring, to a location where a visible and/or audio alarm would be activated at a console. This console would provide information that would identify the classroom where the panic button was activated, but not who activated it. A more advanced system may incorporate the PA system, which allows the teacher and the administrative personnel to hold a two-way conversation by using the existing room PA speakers and installed internal wiring. The cost of this system for an average school would be approximately \$10,000.

There are several weaknesses to a panic-button system. In a classroom situation, it is possible that the panic button would not be readily available in a duress situation. It may be across the room from the teacher's desk or even accidentally blocked by furniture or posters. Also, this configuration lends itself to nuisance alarms triggered by mischievous students. This problem can be offset by hiding the pushbutton or requiring a teacher to enter a PIN on a keypad before use. (The latter is not recommended for schools because of the potential liability of a student attempting, unsuccessfully, to summon help in a threatening situation.) Such a system does not actually identify the person using it, only the owner of the device, but does locate the alarm to a particular classroom or wherever the pushbutton is physically mounted. A panic-button system is cost-effective when installed during the school's initial construction, rather than as a retrofit, and can be a simple and effective system for many types of emergencies.

**A second type** of system incorporates a pager like device that has a panic button built in and is either worn by school personnel or may be installed within a foot switch located under a desk. When the panic button is pushed, a wireless alarm signal is sent to the closest installed wireless sensing unit (a type of repeater) which would then send the signal on to the alarm console. The personnel at the console would receive a coded number and this number would correspond to a teacher. This system does not usually give specific locations other than to the general preprogrammed zone of the repeater. Increasing the number of zones requires more wireless sensing units to be installed, which increases the cost and complexity of the system. A major limiting factor for this system is that the pager like device must have a clear line of sight to the nearest sensing unit for an accurate transmission. In other words, walls, glass, roofs, floors, and so forth will degenerate the transmitted signal which decreases the precision of identifying an individual under duress.

This type of system may also incorporate a two-way radio built into the pager that would allow communication between the console operator and person under duress, but this larger pager is more awkward to wear. Also, if a school has an existing PA system, a duress system could utilize the existing PA system wiring to send the signal from the sensing unit to the alarm console. This hybrid system would use both wireless and preexisting wires to reduce the hardware and installation costs. An estimated cost for this type of system would be about \$50,000.

**A third system**, a smarter version of the previous system, can identify, locate, and track the person who activated the duress alarm of his or her pager. Again, school personnel would push the panic button in a duress situation, and this action would send a wireless alarm signal to a more sophisticated wireless sensing unit. The sensing unit would forward the signal to the alarm console. An extensive wireless infrastructure identifies, locates, and tracks the pager device (and hence the person under duress) within school property. The electronics and software of such a system produces a positioning symbol on a console panel or map like display.

**Advanced and promising technologies:** The Global Positioning Satellite (GPS) technology that is currently identifying, locating, and tracking everything from military soldiers to car rental vehicles has not been shown to be as successful when used inside buildings or around large or tall buildings. GPS requires an unobstructed signal from the ground transmitter unit to an Earth-orbiting satellite. Some advanced duress systems use a hybrid design that tracks outside personnel with GPS technology and RF or infrared systems for tracking personnel inside facilities. The cellular phone system infrastructure is improving greatly in capabilities and coverage, which in the future may be a great asset to duress alarm signals. Advances in low earth-orbiting satellite technology that transmits data may also prove to be beneficial in making duress alarm systems more intelligent in the future.

Duress alarm system technologies are improving at a very fast pace but will likely have to come down substantially in cost before they will be affordable to most schools. Before going out on bid for the purchase of such a system, it is recommended that school administrators communicate with current users or request to participate in a demonstration of the proposed system.