SAND2005-4056
Printed June 2005

DRAFT

NIJ

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

U.S. Department of Justice
National Institute of Justice

U.S. Department of Energy

Sandia National Laboratories

Sandia National Laboratories

National Institute of Justice

The Appropriate and Effective Use of Security Technologies in U.S. Schools — Version 2 —

June, 2005

A Guide for Schools and Law Enforcement Agencies

The Appropriate and Effective Use of Security Technologies in U.S. Schools — Version 2 —

A Guide for Schools and Law Enforcement Agencies

June, 2005

Written and produced
by
Mary W. Green
Sandia National Laboratories

NCJ _____

National Institute of Justice

Sara Hart

Director

Mike O' Shea

Program Monitor

This project was supported under award number 97-IJ-R-072 from the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

1. Foreword

To be from Sara Hart

2. Preface

To be written by Mary Green.

3. Acknowledgments

Written and produced by: Mary W. Green, Sandia National Laboratories, Albuquerque, New Mexico

Original art work by: Phil Wethington, TechReps a division of Ktech Corp., Albuquerque, New Mexico
Elaine Perea, TechReps a division of Ktech Corp., Albuquerque, New Mexico

Photos by: Richard Sparks, Sandia National Laboratories, Albuquerque, New Mexico
Phil Wethington, Tech Reps, Inc., Albuquerque, New Mexico

Document preparation: Elaine Perea, TechReps a division of Ktech Corp., Albuquerque, New Mexico
Debra Rivard, TechReps a division of Ktech Corp., Albuquerque, New Mexico

Technical contributors: Betty Biringer, Sandia National Laboratories, Albuquerque, New Mexico
Richard Sparks
Tim Malone
Dale Murray
Charles Ringler
Dave Furgal
Larry Wright

Library research: Kay Kelly, Albuquerque, New Mexico

Reviewers: Betty Biringer, Sandia National Laboratories, Albuquerque, New Mexico
Richard Sparks
John Kane
Basil Steele
Bob Waters
[to be added to as reviews are completed]

This manual is dedicated to the excellent administrative staff at Permian High School in Odessa, Texas.

Contents

Chapter I
Fundamental Concepts for Security in Schools

The purpose of this report is to provide school administrators with the ability to determine their security system requirements, so they can make informed decisions when working with vendors and others to improve their security posture. This is accomplished by (1) explaining a systems-based approach to defining the objectives and needs of the system, and (2), providing information on the ability of common components (sensors, cameras, metal detectors, etc) to achieve those objectives, in an effectively integrated system. This chapter presents some fundamental security concepts, preparatory to ensuing chapters, including

1. The purpose of security technology in schools
2. A systems approach to security
3. Security system functions
4. Effective security measures used today
5. Order maintenance
6. New school designs

Much of the guidance provided in this work is the result of Sandia National Laboratories' extensive experience in solving security-related problems and conducting security risk assessments for a wide range of facilities around the world. These concepts have been incorporated at selected "pilot" schools throughout the United States to demonstrate appropriate and effective implementation of security technologies.

1.1 The purpose of security technology in schools

The purpose of implementing security technologies in schools is to increase the security and safety of (or reduce the risk to) students, staff, and school assets, and to prevent major disruptions to teaching and learning. Specifically, security technology can

1. Compliment existing policies and procedures, and assist staff in enforcing them
2. Increase the likelihood of catching and identifying offenders
3. Discourage further security infractions
4. Reduce or eliminate the opportunities to commit security infractions.

Some schools with security problems have simply increased the number of adults (or security staff) on campus in an effort to increase the likelihood of catching offenders, or to deter them from committing offenses. However, adding professional security staff to perform very routine security functions has many limitations:

- Manpower costs are always increasing
- Locating qualified people willing to work only a few hours a day can be difficult
- Turnover of security personnel is common-place and detrimental to a school security program
- Repetitious or mundane tasks can be boring and a threat to employee morale as well as productivity

Many school administrators reported that they would like to discourage security infractions (such as theft, vandalism, assault, false fire-alarm pulls, etc.) by means of any deterrent available to them. In our experience, deterring most people is best achieved when the school has an excellent reputation for security. That is, whenever an incident occurs, the person is identified and punished due to the robustness and effectiveness of the school's security system. This means that

1. The security system must have a HIGH likelihood that a person will be caught (and/or sufficient evidence will be collected to correctly identify that person), and
2. There will be unpleasant disciplinary action or even prosecution as a result.

Additionally, if students, staff, and the community are aware of the system's successes, a reputation develops that tends to deter those who fear the consequences. Deterrence is not achieved through the mere presence of security features (such as a sign that indicates "Trespassers will be prosecuted") or technologies, but through the integration of those features and technologies into a system that accomplishes items 1 and 2 above.

Additionally, school districts may be held accountable for unfortunate incidents that occur in their schools. For example, a number of schools in this country have seen lawsuits or even an exodus of students when they were perceived as not being safe or secure. This type of problem perpetuates

upon itself, as a reduced student population garners less revenue, and less revenue means poorer services to the remaining students, thereby reinforcing negative perceptions. It is therefore necessary to document

1. The process that was used to determine security needs, and
2. That all reasonable effective and appropriate steps to ensure security are carefully planned and implemented

Many of these steps can be conducted or enhanced by the technologies presented in Chapters 3 through 6 of this report, following the structured approach described in chapter 2.

1.2 A systems approach to security

Too often in schools, like many businesses, security technology innovations are not applied effectively, are expected to do more than they are actually capable of, and are not well maintained after the initial installation. In such cases, security technology can be a waste of time and resources. A significant number of schools have been less than pleased with the ultimate cost, maintenance requirements, and effectiveness of security products they have purchased. In our experience, some of the difficulties contributing to these problems are that

- Schools rarely have detailed knowledge, training or experience in security technologies
- Schools do not usually have the funding for aggressive and extensive security programs
- Many schools cannot afford to hire a security technology consultant
- Schools usually lack the expertise to maintain or upgrade security devices – when something breaks, it can be difficult to have it quickly repaired or replaced
- Privacy issues or potential civil rights lawsuits may complicate the implementation of some technologies, especially in districts where no precedent exists for using them.

In the past, schools have rarely considered their security plans from a systems perspective — looking at the big picture of what they are trying to achieve in order to arrive at an optimal security strategy. Too often, a school's security strategy is really a compilation of many independent decisions that were driven by unrelated security problems. This has resulted in disjointed and occasionally illogical security measures. A systems approach is required to develop a well thought-out security program that integrates all the elements (such as policies, procedures, hardware, software, and personnel). This allows schools to document the security decisions and allocation of security resources.

A systems approach considers all factors that affect the way security will be accomplished, such as:

1. What are the operating constraints of the school (the characterization of the facility)?
2. Who or what is the school trying to protect (that is, what assets or activities)?

3. Against whom should they be protected (i.e., the threats, or perpetrators)?
4. What are the possible undesirable events of concern carried out by the categories of threats?
5. What is the likelihood of each event, and if it occurs, what is the impact or consequence?
6. What weaknesses in the system need to be corrected, and what upgrades will best improve them?

A brief overview of the approach is presented here and discussed in greater detail in Chapter 2.

School characterization

Every school is unique in construction, population, staff, demographics, layout, policies, relationships with local law enforcement, security problems, etc. To completely characterize the school it is important to gather enough information through site maps, a thorough understanding of all operational constraints, historical data on security incidents, and input from all stakeholders regarding current security concerns.

Asset identification

The locations, actions or assets to protect are often identified by considering what **undesirable events** might occur at the school and then extracting from these events the associated locations, activities or assets needing protection. For example, a false fire-alarm pull, a weapon on campus, theft of student organization monies, assault, or natural disasters are all possible undesirable events. Administrators can also ask, "Which assets are most at risk?" The protection of students and staff is always at the top of this list. Are the instruments in the band hall attractive targets for theft or vandalism? Is the new computer lab full of the most current and re-sellable computers? Are staff vehicles frequently vandalized?

Threat identification

A school's threats (perpetrators) must also be identified because they act out the undesirable events. For example, who is your school currently most threatened by:

- Outsiders (drug dealers, students from rival schools, terrorists, irate parents, criminals, psychotic individuals, gang members)?
- Insiders (disgruntled teachers, maintenance or custodial staff; volatile or unstable students; etc)
- Other (Extreme weather or natural disasters)?

Administrators should consider what they know or expect of those perpetrators: How sophisticated are they? Do they have tools or knowledge that helps them accomplish their malevolent activity? What are their motives? Are they willing to risk being caught or injured?

Likelihood and consequence of undesirable events

Some possible undesirable events at a school might include

- Gang rivalry or violence on campus
- Fights behind the gym
- Drugs hidden in lockers
- Guns brought to school
- Outsiders on campus

- Drinking at lunchtime
- Vehicle break-ins
- Graffiti in the bathrooms

Undesirable events must be analyzed to determine their likelihood and consequences (impact), so they can be prioritized. Prioritization helps administrators decide which of these risks are acceptable, and which risks might be reduced by implementing security measures.

Risk management – balancing performance, cost and risk

Once the assets to protect are identified, the threats evaluated, and the risks are prioritized, risk management techniques are applied to determine suitable solutions to perceived vulnerabilities. Risk management is the process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost and performance (Jaeger, 2003). Tradeoffs between performance, cost and risk must be made, because no facility, especially schools, can afford to protect against all possible threats. Further, it is not fiscally feasible for schools to protect all assets or activities with the same level of protection.

School districts must therefore carefully decide which security strategy is most reasonable for each undesirable event, and implement the appropriate measures. The result is a carefully planned strategy combining technology, personnel, and procedures that best addresses security problems within financial, logistical, and political constraints. There is no single security strategy or system that will work ideally across all schools. Additionally, a school's security program may need frequent revision with changes in constraints and the asset/threat mix.

Security system functions

An appealing goal in any school security program is to deter the perpetrator from doing whatever it is he is considering. This tends to be accomplished if the action is perceived as too difficult, no longer worthwhile, or the chances of being caught are too high and consequences are too undesirable (such as jail time or exclusion from participation in school sports programs). Deterrence is the natural result of an effective, integrated security program that detects, delays, responds to, apprehends, and prosecutes offenders. Part of the risk management process is to examine possible solutions to vulnerabilities from the perspective of these system functions. If these functions do not occur, there is little or no deterrence value to the system.

For example, if your school posts a sign stating trespassers will be prosecuted, but it is well-known that trespassers are rarely prosecuted (perhaps because they are rarely detected and apprehended) then the sign has little if any deterrence value. It might keep good people good, but means nothing to would-be offenders. Conversely, if it is well-known that trespassers are frequently apprehended and prosecuted (because this has historically been the

case), the sign tends to have higher deterrence value against those who are unwilling to risk getting caught.

Schools have several choices regarding strategies for dealing with the various security risks they face. The three general protection strategies are Prevent, Apprehend, or Mitigate. The primary functions of a security system whose protection objective is to truly *prevent* an undesirable event are (Garcia, 2003):

1. Detect that an adversary in the process of attempting a malevolent act
2. Communicate the detection information to the appropriate personnel
3. Delay the adversary from completing the undesirable event until response can arrive
4. Response by security personnel to interrupt and prevent completion of the event

For example, when someone is breaking into a building, it is necessary to detect the intrusion and send notification to a response force as soon as possible. Next, this adversary must be delayed (slowed down) so that there is enough time to respond before the intruder accomplishes his task and escapes. (A simple example of delay is to firmly bolt school computers to large heavy desks, so that a thief is forced to use more time removing the bolts.) The response personnel, such as the police, or a contract guard must physically respond and arrest the adversary before he escapes with the computer.

Alternatively, a prevention strategy can be accomplished through a single function, Remove the opportunity. This function prevents an undesirable event by making it impossible to accomplish (for instance, by removing a statue that is frequently vandalized).

Schools may not be capable of implementing a prevention strategy for many undesirable events. For instance, schools may lack the resources for real-time response to many types of security incidents (such as night time break-ins or vandalism), and delay of the adversary is simply not possible in some incidents (i.e. fighting, drugs in lockers, assault, trespassing, etc.). After-the-fact investigation is often the best a school can hope for. In these instances an *apprehend* strategy may be more appropriate. The primary functions of an apprehend strategy are

1. Detect the event has occurred
2. Communicate the detection information to the appropriate personnel;
3. Apprehend the adversary, or *collect evidence* sufficient to identify the perpetrator and apprehend at a later time
4. Prosecute / discipline the adversary

A school might use this strategy to aid in deterring and resolving fights that occur on campus. Once it is known the fight has occurred evidence is collected by reviewing footage recorded via installed video cameras. The evidence hopefully identifies who

participated and who is at fault in the incident. Guilty parties are then apprehended and appropriately prosecuted or disciplined.

Both *prevent* and *apprehend* strategies can result in deterrence if the system effectively performs the required functions above, but only for those individuals who are deterred by the consequences of their actions. For instance, it may not be feasible for schools to attempt a prevention or apprehension strategy for suicide attackers, bomb threats, drive-by shootings, or terrorism. These undesirable events are extremely rare, extremely hard to prevent, and hard to deter. Sometimes the best a security system can do is to mitigate the consequences of an event. The functions of a mitigation strategy are

1. *Communicate* or *notify* the appropriate personnel that a crisis is in process;
2. *Assess* the situation, if necessary;
3. *Initiate* the appropriate *emergency procedures;*
4. *Optimize* the r*esponse effectiveness*

Finally, schools might choose to not implement any strategies or security measures for particular undesirable events. It simply may not be feasible to attempt to reduce the risk associated with them. There will be limited resources and it may be necessary to accept the risk associated with some events.

Security measures under consideration should be systematically assessed according to their ability to perform the functions associated with the selected protection objective. This model is recommended because its use has proven effective over many years. Using the above model can also prevent the implementation of less effective security strategies. For example, a large urban high school with which the authors are familiar was planning to purchase $100,000 of exterior cameras to combat nighttime vandalism on the exterior of the building. This plan was halted abruptly when the administrators were questioned as to who would be available to watch the monitors (the **detection**) from the 40 cameras, and who would respond quickly enough to these sporadic and infrequent incidents (the **response**). A low-cost (and more effective) alternative was devised that incorporated anti-graffiti sealer on all brick surfaces, strategically located wrought iron fencing that could not be climbed easily, and replacement of particularly vulnerable windows with glass block.

1.4 A spectrum of available countermeasures

A wide array of security measures involving people, campus modifications, and/or technologies are possible today, though the application will vary with the unique characteristics of each school. Figure 1.1 presents some of the security features available for use against various undesirable events. This list assumes that schools have already established appropriate consequences for the perpetrators of undesirable events. Otherwise, there is little or no deterrence to be

gained from any physical security measures designed to detect, delay, and respond to an incident. Schools currently considering any of the measures listed in Figure 1.1 should systematically assess them according to their ability to perform the functions associated with the selected protection objective (discussed above and in Chapter 2). Additionally, a school should always contact its legal counsel before participating in any new security program that involves the searching, oversight, or testing of people or property.

A recurring message from school administrators is that the majority of their problems are brought onto campus by outsiders or expelled/suspended students. Therefore, the measures presented here that are designed to keep outsiders off campus will generally be of global interest.

1.5 New school designs

Many school buildings in the United States have been constructed to achieve an inviting and open feeling. They feature multiple buildings, large windows, multiple entrances and exits, and many areas for privacy when study or reading. These layouts have generally been developed without considering security concerns. To combat broken windows and nighttime thefts, the country also went through a brief period of designing schools with almost no windows. The cave-like results these designs produced were quickly found to be objectionable to most people. Many schools will be forced to work with their existing campus and infrastructure.

If a school district has the luxury of building a new school, security should be one of the factors considered during the design phase. It is important to involve trained security personnel in the design to help address likely security problems the school will face. Additionally, there are architectural firms specializing in schools that incorporate good security principles. Incorporating the principles of Crime Prevention Through Environmental Design (CPTED) in the design or remodeling of a school can contribute to the security of a campus (Crowe, 2000).

A security-conscious design can actually help compensate in the long term for tight security budgets, fewer security personnel, and less-sophisticated security equipment. The funding, location, geography, expected threats, available space, security objectives and community characteristics will drive which CPTED ideas are feasible for each new school. The following is a list of items to consider when designing a new school. These considerations are based on the authors' experience and CPTED concepts, and may enhance security in the design of new schools. Please note that there are alternative views and/or tradeoffs associated with these recommendations, as noted below, depending on the situation and objectives for the new school design.

Undesirable Event	Potential Countermeasures
Outsiders on Campus	Posted signs regarding penalties for trespassing
	Enclosing the campus with attractive shrubbery and climb-resistant fencing
	Guard at main entry gate to campus to validate identification
	Greeters in strategic locations
	Student I.D.s or badges worn on top of clothing
	Vehicle parking stickers
	Uniforms, standard attire, or dress codes
	Locking all or most exterior doors from the outside
	ID check for anyone in hallways during class
	Cameras in remote locations
	School laid out so all visitors must pass through front office
	Temporary, self expiring badges issued to all visitors
Fighting or assaults	Video cameras in common gathering areas
	Duress alarms
	Whistles
	Adults throughout the camps during non-class time
Vandalism	Graffiti-resistant sealers for vulnerable surfaces
	Glass-break sensors near banks of windows
	Aesthetic wall murals (these usually are not hit by graffiti)
	Law enforcement officers living on campus
	8-foot, climb-resistant fencing or Pyracantha bushes (see Figure 1.2)

Figure 1.1 A sample listing of some undesirable events, and countermeasures currently in use against them.

(Note: Though most of these suggested security measures are used in U.S. schools today, documented information regarding their effectiveness DOES NOT yet exist. More research is needed to reveal the statistical effectiveness of these measures and technologies. Current effectiveness is based on anecdotal evidence. Further, none of these measures should be implemented without folowing the process outlined in Chapter 2.)

Vandalism cont'd	Well-lit campus at night and exterior lighting that is controlled by motion sensor devices (see Figure 1.3)
Theft	Interior intrusion detection sensors
	Property marking to deter theft (see Figure 1.4)
	Bars on Windows
	Reinforced doors
	Elimination of access to rooftops (Figure 1.5 and 1.6)
	Cameras in areas with high-value assets
	Doors with hinge pins on the secure side
	Bolting down computers and TVs
	Placing high-value assets in interior rooms
	Key control
	Biometric entry into rooms with high-value assets
	Law enforcement officer living on campus
Drugs	Drug detection swipe kits
	Hair analysis kit for drug use detection (usually intended for parental application)
	Drug sniffing dogs
	Complete removal of lockers
	Random searches of lockers, backpacks, and student/staff vehicles
Alcohol	No open campus during lunch
	Alcohol breath testing equipment available to the school
	No access to vehicles during the day
	No lockers
	Allowing only clear or open mesh backpacks
	Saliva test kits to be administered by the school nurse
Weapons	Walk-through metal detectors
	Hand-held metal detectors
	Crime-stopper hotlines with rewards for information
	Gunpowder detection swipe kits
	Random locker, backpack, and vehicle searches
	X-ray inspection of backpacks and purses upon entry to school

Parking lot problems	Cameras
	Parking decals
	Fencing to prevent wide and unsupervised access to parking lots
	Card I.D. systems for parking lot entry
	Partitioning parking lots for different student schedules, each of which is kept locked until access is required
	Sensors in 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 (see Figure 1.7)
	Boxes installed over alarm pulls that alarm locally (a.k.a. screamer boxes)
Bomb threats	Caller I.D. on office/lobby phone system
	Crime-stopper hot-line program with attractive rewards for information
	Recording all inbound phone calls, with a greeting message played at the beginning of each incoming call
	All incoming calls routed through a district office
	Phone company assistance in tracing calls
	No pay phones on campus
	Policy to extend the school year an appropriate amount of time when plagued with bomb threats and subsequent evacuations
Bus problems	Video cameras and recorders within enclosures on buses
	I.D.s required to get on school 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

Figure 1.2 Pyracantha bushes can create an intimidating barrier where fences might be inappropriate. Use caution when locating these types of barriers so that convenient hiding places for contraband are not created.

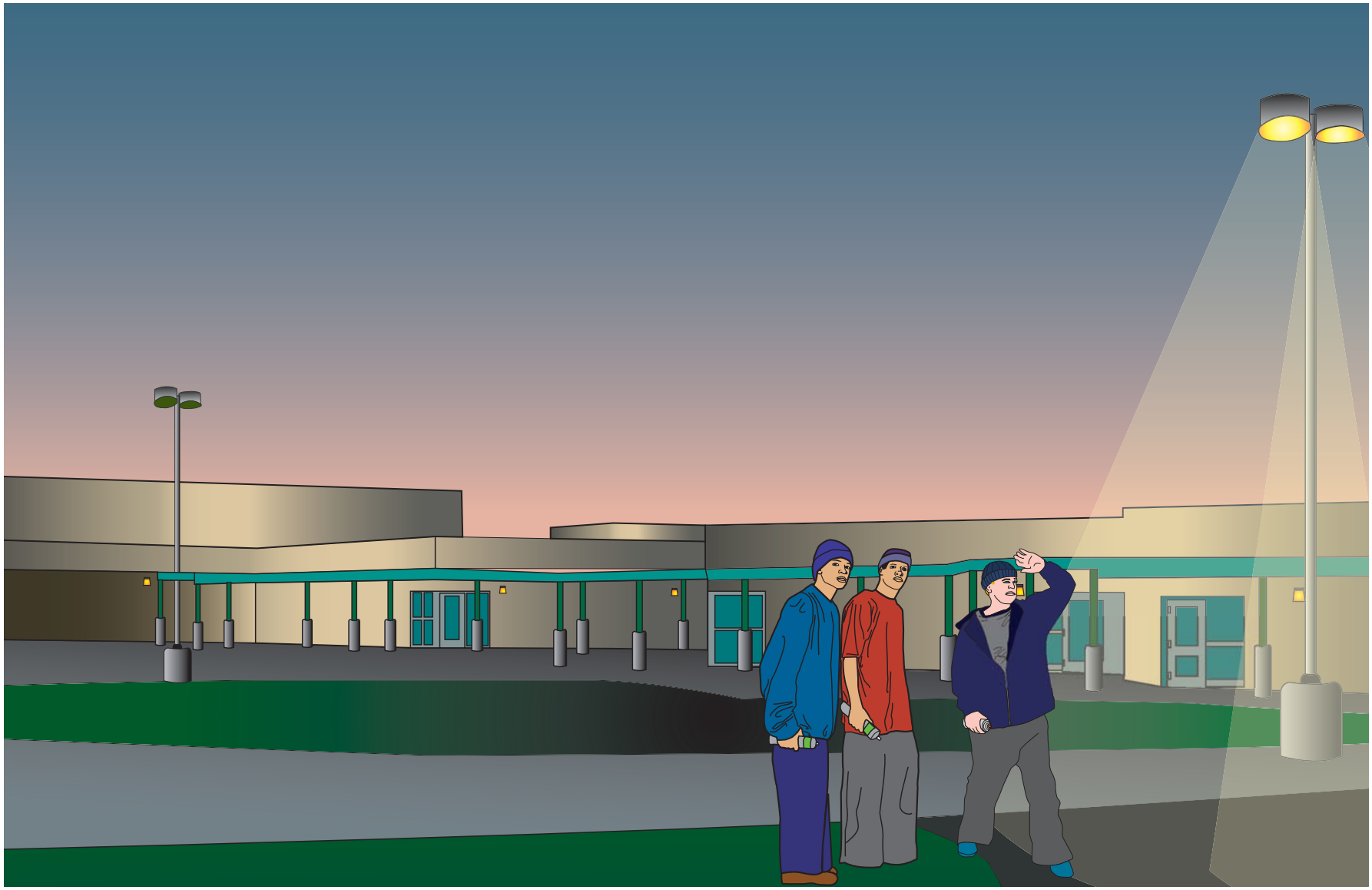


Figure 1.3 ***Some exterior lighting may be connected to a simple motion detection device; this may serve as a deterrence to would-be vandals. Close neighbors may even be happy to contact the authorities when they notice unusual nighttime visitors.***

Figure 1.4 Marking school property can reduce its attractiveness to would-be thieves by reducing as the potential resale value in the stolen goods market.

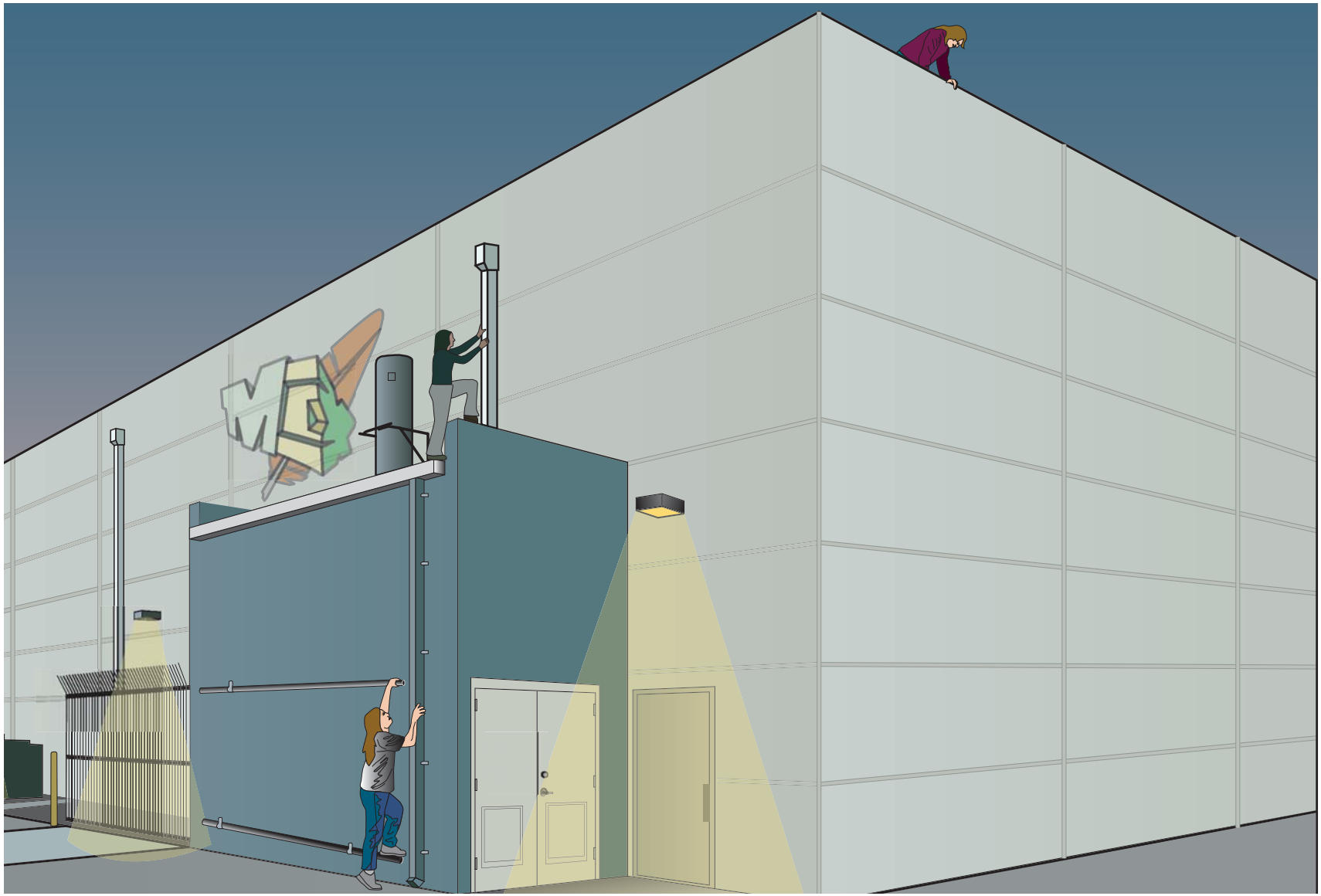


Figure 1.5 Exposed utility conduits, drain pipes, or facility support structures may provide easy access to a school's roof, creating opportunities for theft (through skylights,) or vandalism, as well as a liability concern if a student were to fall off.

Figure 1.6 ***When maintenance ran new electrical lines around this school campus, they created a very simple way for students to climb onto this roof. One solution to this particular situation is to build some type of barrier or enclose the offending structure above six or seven feet from the ground.***

Figure 1.7 ***Preventing false fire alarm pulls in some schools can become a full-time job. Some new fire alarm systems allow school staff to investigate an alarm pull before the alarm becomes audible and evacuations take place.***

1. Minimize the number of buildings and entrances to the school to support efforts to keep outsiders off campus. Alarm other exits for emergency use only. One tradeoff is that there may be few entrances for police or other response forces to quickly enter during a disaster (such as a terrorist, hostage situation, or medical emergency).
2. Allow enough space at the main entry in the event that a screening area (such as for weapon or drug detection) is implemented later on.
3. Post a security person or other greeter at a single vehicle entrance onto campus. This allows you to challenge each vehicle for identification and verification of all occupants as students, but may reduce throughput at peak arrival times. Buses and school employees should have a separate (and controlled) entrance.
4. Keep the school well-maintained and litter-free to increase a school's order maintenance (see Section 1.6).
5. Locate the staff parking lot such that students will not normally traverse that area. This may inconvenience staff but is intended to reduce the opportunity for vandalism.
6. Enclose the campus with attractive (but difficult to climb) fencing and shrubbery. This explicitly defines property boundaries and forces perpetrators to consciously trespass, rather than gain casual entry (see Section 4.1).
7. Minimize secluded hiding places for unauthorized persons, both inside and outside buildings on campus. This is a tradeoff because alcoves create privacy for studying as well as mischief. Additionally, they might serve as a hardened fighting position for either the police or an adversary during an armed conflict.
8. Use windows strategically. Consider incorporating clerestories or secure skylights that allow light in but are less vulnerable than typical windows. Having many windows yields a lot of light and is aesthetically pleasing but makes a school easier to break into; having few windows is confining and cold, but generally creates a more secure building.
9. Large wide spaces, like hallways or common areas, should have sufficient vertical and horizontal dimensions so that the space does not feel uncomfortably restrictive to students. Large, wide hallways provide easy traversal and clear line-of-sight for monitoring students, but also provide clear line-of sight for armed adversaries.
10. Consider installing student lockers in classrooms, the cafeteria, or in other areas that are easy to monitor so no single locker area becomes a bottleneck, and there is always the deterrence of an adult nearby (see Figure 1.8).
11. Make certain that your facility has built in the necessary receivers, transmitters and repeaters throughout the structure to allow dependable

two-way radio and/or cellular communication. This however is difficult to do without first testing the equipment at the intended facility to determine if the performance is satisfactory.

12. Install sensors or alarm systems throughout hallways, administrative offices, and rooms containing high-value property, such as computers, VCRs, shop equipment, laboratory supplies, and musical instruments.
13. Consider allowing a law enforcement officer to live on campus. A police vehicle parked on campus during nights and weekends can serve as a deterrent. Such an arrangement can provide response to intrusion sensor alarms and detection (albeit minimal detection) and response in situations where an alarm is not used (Figure 1.9).
14. 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.
15. Make certain that exterior lighting is sufficient for any external night time cameras that may be employed.

1.6 Order maintenance

One additional consideration is the perception that a school is well under control with responsible and vigilant supervision. This state of control is often referred to as "order maintenance". If a school is perceived as unsafe (that is, it appears no authority prevails on a campus), then undesirable events (such as vandalism, theft or assault) are more likely to occur, and the school may actually become unsafe. This is an embodiment of the "broken window theory": one broken window left unrepaired will encourage additional broken windows. Seemingly small incidents of vandalism, litter on campus and buildings in disrepair may promote a negative reputation and perception of the school. A possible result is loss of community confidence.

Issues contributing to a school's overall order maintenance must, therefore, be taken seriously, as with any public facility. Reducing theft, deterring vandalism and graffiti, keeping outsiders off campus, keeping facilities in good repair, improving poor exterior lighting, maintaining attractive landscaping, and getting rid of trash are ways to improve order maintenance, and promote security in schools (see Figure 1.10). Technologies such as cameras, sensors, and ID badges presented in this report may help maintain order maintenance.

In the authors' experience, school districts often under-value 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. The janitorial staff should be selected with care because they have great access to and knowledge of staff, students and school assets. Some school

Figure 1.8 Crowded hallways that also house student lockers can create a hostile situation between students.

Figure 1.9 ***Would anyone be aware of malicious activities occurring at your school during off hours? This "senior prank" destroyed more than 20 trees at this high school. If a police officer lived on campus, the sound of chainsaws may have been noticed and interrupted.***

Figure 1.10 Keeping a school well maintained and litter free is critical to a school's order maintenance.

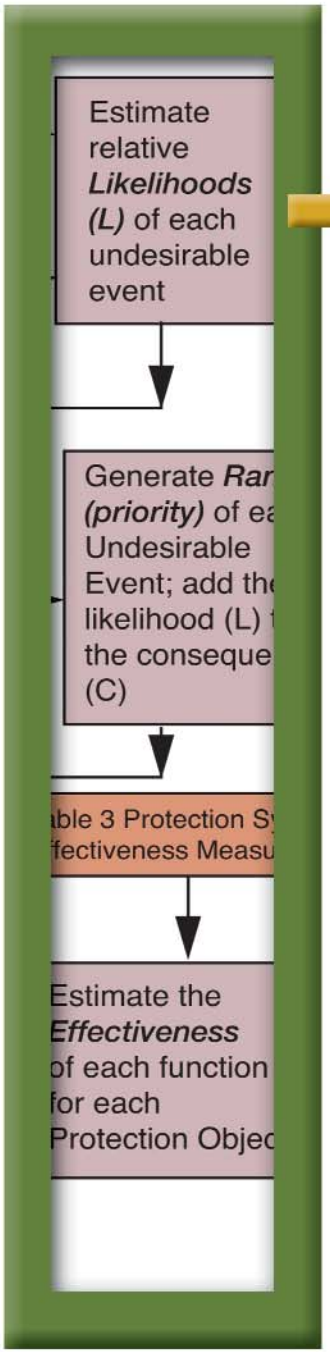
districts have saved money through contracts with janitorial service providers. While this may be accomplished successfully, it can yield

- High turnover of cleaning personnel, due to low wages paid to the workers
- Cleaning personnel who have not been appropriately screened before hiring with complete background checks
- A greater chance of pilfering, especially at night, when there is a high-turnover of cleaning personnel
- A potential decrease in the quality of the cleaning, since contract personnel know that they are only temporary and may not take any pride-of-ownership in their work.

Making a school's cleaning crew an integral part of the school staff can increase the pride this crew takes in their work.

References

1. Crowe, T.D., National Crime Prevention Institute, Crime Prevention Through Environmental Design, Boston, Butterworth-Heinemann, 2000.
2. Garcia, M.L., The Design and Evaluation of Physical Protection Systems. Boston: Butterworth-Heinemann, 2001, p53.
3. Jaeger, C. D., "Security risk assessment methodology for communities (RAM-C)", SAND2003-4766C, p 1-4.



Chapter II
Systematic Methods to Prioritize and Address Security Risks

School administrators must decide how to allocate their limited security resources. For example, suppose that at Main Street High School, the principal assigns the bulk of the security personnel and teachers on duty each morning to the bus drop-off area and the student parking lot. At the first tardy bell, some of these personnel are reassigned to gather late students left in the hallways, herd them to the front office for tardy slips, and then escort them to class. When the first lunch bell rings, security personnel oversee the cafeteria, main hallway bathrooms, and the area behind the gym.

The principal has set his priorities based on a combination of

- Recent problems at his school,
- What staff members are telling him they believe is occurring at the school, and
- His own concerns about what could potentially happen.

In the morning, he wants to prevent cars from being “keyed”, students from fighting in the parking lot, outsiders from selling drugs, and parents from weaving their vehicles between buses to avoid the slower car traffic lane. After the tardy bell rings, he wants to discourage students from deciding to skip class rather than be late. He is aware that during the lunch period, there is bullying in the restrooms and students have been caught smoking pot behind the gym.

The principal has assigned personnel where he believes they will be the most effective. Perhaps any administrator in his place would have allocated security resources in the

same way, if given the same knowledge of the students and incident history. After all, no school can protect against all possible security incidents that could occur – there simply are not enough resources. But how can administrators make defensible decisions about how to allocate scarce security resources?

Administrators and security teams can use a standardized and systematic approach to identify, prioritize, and then address the range of possible incidents at their school. The approach should help them determine

1. Which incidents are most important to protect against, and who is likely to carry out these incidents
2. What vulnerabilities in the system prevent the school from effectively protecting against each of these incidents, and
3. Which security measures to implement in order to arrive at an acceptable level of risk (i.e., how much risk to accept)

Such an approach will result in the most reasonable (and defendable) decisions as to how limited security resources are applied. Furthermore, it provides a traceable, documented record of why particular decisions were made, and demonstrates that these results are repeatable.

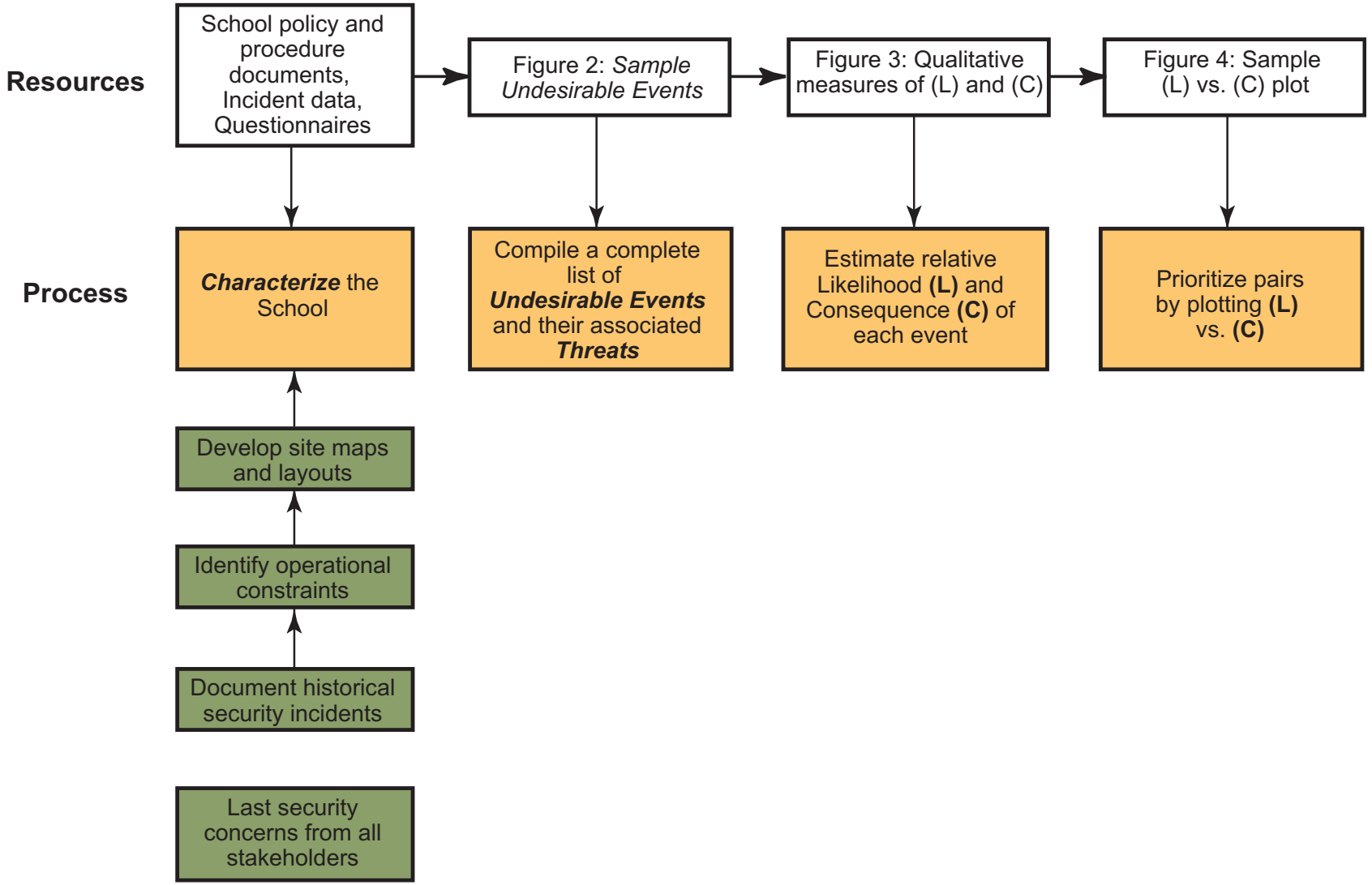
This chapter discusses one method, based on risk, to help schools identify and prioritize undesirable events they want to prevent. This discussion is followed by a systematic approach for evaluating and addressing security vulnerabilities associated with those undesirable events. Finally, a discussion on the importance of contingency plans for periods of heightened security risks is presented.

These analytical approaches to school security are based on many years of national laboratory experience in successfully improving security at multiple civilian infrastructure sites (Biringer, 2000; Biringer and Danneels, 2000; Jaeger, 2002; Jaeger, 2003; Garcia, 2001; Matalucci, 2002). Using these approaches will help change the "art" of school security into more of a science, provide a rational framework for funding security enhancements, and help administrators make the best possible security decisions.

2.1 Identifying and Prioritizing Security Risks

This section presents one method to identify and prioritize a school's security risks that results in a traceable and documented assessment of security needs. There are of course other ways for schools to determine what incidents are most important to them (that is, what they most want to protect against). The risk assessment methodology selected should be a systematic process that assesses security vulnerabilities and makes decisions based on risk. Figure 2.1 shows the method described in this report.

The steps consist of (1) characterizing the school and its environment, (2), developing a


Resources
Process
School policy and procedure documents, Incident data, Questionnaires
Figure 2: *Sample Undesirable Events*
Figure 3: Qualitative measures of (L) and (C)
Figure 4: Sample (L) vs. (C) plot
Characterize the School
Compile a complete list of ***Undesirable Events*** and their associated ***Threats***
Estimate relative Likelihood **(L)** and Consequence **(C)** of each event
Prioritize pairs by plotting **(L)** vs. **(C)**
Develop site maps and layouts
Identify operational constraints
Document historical security incidents
Last security concerns from all stakeholders

comprehensive list of undesirable events and their associated threats, (3), estimating the likelihood and consequences of these events, and (4) rank-ordering the undesirable events. This type of approach helps schools prioritize the assets, areas, and activities they wish to protect, and decide how well to protect them. This information can also be used to determine how to improve any weaknesses in the system.

Characterize the School

A fundamental step toward identifying the top security priorities of a school is to characterize the school and its security environment. This usually consists of collecting four groups of information: a detailed site map; a thorough understanding of all operational constraints; a list of historical security incidents; and input from all stakeholders on current security concerns.

To characterize the school, first obtain updated maps of the school and campus. Site maps are vital to characterizing the school, and should clearly illustrate all areas of campus. They should be easy for security or emergency response teams to read and understand. Some types of information that should be included on the maps are:

- The floor plans of all buildings, labeled with room numbers and the teachers assigned in each room,
- Stairwells, utility rooms, closets, and exterior and interior doors,
- Parking lots, driveways, and sidewalks,
- Gates, fences and fencing materials (such as wrought iron, chain link, brick, etc.),
- Utility locations, including air and water intake,
- Portable buildings, outbuildings and athletic fields,
- Any installed security equipment (sensors, alarms, etc.), and
- Assembly areas for emergency evacuations

Second, the ***operational constraints*** and philosophies that influence how security is accomplished must be well understood, and this will be unique to each school. This information will constrain or allow various security upgrades or enhancements. For example,

- Are teachers allowed to enter the school building at any time and do they have their own keys to do so?
- When do the janitorial crews do their work? Do they have keys and to which doors? Do they set the alarm system while they work or after they leave?
- Do you use professional security guards, teachers, both, or neither to enforce security? Has your school organized a security team? If so, how is it organized, and what are its roles and responsibilities?

- Where are the security guards (or team members) generally located, and how long does it take them to respond when summoned?
- Which exterior doors are unlocked during the day, and is this subject to be changed as needed?
- Do groups other school-sponsored organizations use any of the school's buildings or grounds and when? Are they required to furnish security?
- Which doors are visitors supposed to use to enter the school; what doors are visitors able to use to enter a school building? How is visitor control enforced? What are the procedures they must follow?
- Are police allowed to carry firearms on campus during school hours?

(This might be a good time to re-think or upgrade some of these constraints that are no longer optimal for the school's day-to-day business.)

Third, compile a list of all ***historical security incidents*** that have occurred on campus over the last two or three years, and list, using a rough categorization, who instigated each incident. Some example categories are: student, staff member, maintenance, parent, ex-employee, ex-student, criminal, psychotic individual, or gang member. (These categories are known as the "threats" in the security industry. The "threat" is the adversary, attacker or persons perpetrating the incident.) This information is needed to estimate what future events might occur, based on historical incident data, and who might carry them out. This may require gathering of data from multiple sources, including the school (for simple misconduct incidents), the district (for incidents requiring suspension), and the local police (who might keep records of prosecutable offenses). These sources may or may not overlap, which will influence the incident list and tally, if the collector is unaware of which sources are collecting which information.

Also, note any incidents of very serious consequences that occurred before this time period which are still remembered by many staff and/or students. This might also include security incidents of local, regional, national or international notoriety that are cause for concern at your school. For example, slayings and hostage or terrorist situations similar to that experienced Columbine High School (April 1999) or Belsan School in Russia (September, 2004) might be included.

Fourth, develop a comprehensive list of ***security concerns*** from all stakeholders, including teachers, students, administrators, and security personnel. What are their primary security concerns? What do they feel threatens the school's continued safety? How effectively do they feel these concerns are being handled today? A sample set of questionnaires is included in Appendix A, which can be used to help collect these safety concerns.

Identify Undesirable Events and their Associated Threats

Once the four sets of information above are collected, the security team should meet together to review and discuss the third and fourth sets (historical security incidents and security concerns gathered from stakeholders). The team should compile a list of all credible security incidents and associated threats that they expect could occur at the school. This compilation is known as the school's ***Undesirable Events/Associated Threats*** and each entry will be referred to as an "Undesirable Event/Threat pair". The list should only contain undesirable events related to security. For example, truancy or students skipping classes is an undesirable event, but not necessarily a security concern at many schools. (Note: The other two sets of information collected, the campus layout/map and the comprehensive knowledge of operational constraints, are used in subsequent sections of this chapter.)

An example list of Undesirable Event/Threat pairs that may be credible in a school setting is shown in Figure 2.2. This list may help a security team put together their own list more quickly. Not every Undesirable Event is possible at every school, due to varying operational constraints, campus layout, the location, or existing security procedures. Likewise, not every type of Threat (adversary) is credible at every school. Each school should develop their own unique list of Undesirable Events/Associated Threats.

Estimate the Likelihood (L) and Consequence (C) of each Undesirable Event/Threat Pair

It would be difficult to decide what to protect if all of the undesirable events were equally likely, or produced similar consequences. But this is certainly not the case, as some events may be highly likely (such as graffiti), moderately likely (such as a nighttime break-in), or extremely unlikely (such as a terrorist attack). Similarly, the consequence of a particular undesirable event might be minor (such as shaving cream in the boys' bathroom, which is easily cleaned) or far-reaching, such as debilitating injuries to a staff member. Clearly, fewer resources should be spent preventing an unlikely event with insignificant consequences. Likewise, more resources are necessary to prevent events that are likely and serious in consequence.

Estimate the relative likelihood (L) of each Undesirable Event/Threat pair under consideration. The estimates are not actual probabilities of occurrence, but *qualitative measures* of likelihood. The first row of Figure 2.3 shows an example range of qualitative measures for likelihood. You should develop your own qualitative measures or use the example measures provided in Figure 2.3 which uses *Extremely-Low, Low, Medium-Low, Medium, Medium-High, High,* and *Extremely-High* as the range of likelihood. You might only use a simplified subset of these measures (such as Low, Medium, and High). However, this kind of simplification produces less stratification making it more difficult to prioritize the events.

Sample Undesirable Events (Attacks)

1. School property
   a. Theft (daytime, nighttime, off-hours, weekends and holidays)
   b. Vandalism (daytime, nighttime, off-hours, weekends and holidays)
2. Student property
   a. Locker break-ins
   b. Vandalism/theft of student vehicles
   c. Robbery
3. Use of weapons on campus
4. Bomb threat (hoax or real)
5. False fire-alarm pull
6. Fighting
   a. On campus, during school hours
   b. On campus, after-hours, during school-sponsored activities
7. Bullying
8. Drugs brought onto campus
9. Assault/rape
   a. Of Employee
   b. Of Student
10. Sniper/Drive-by shooter
11. Employee molests a student
12. Abduction of a child
    a. By a non-custodial parent or other relative
    b. By an outsider
13. Hacking into student records
14. Attack on the school (with weapons)
    a. Random malevolence
    b. Hostage situation (single room or area)
    c. Complete take-over
15. Natural disasters (flood, hurricane, earthquake, tornado, etc)

Sample Threats (Adversaries) to a School

1. Insiders (individuals who belong on campus or have authority to be there)
   a. Students
   b. Employees
   c. Parents (such as volunteers) and relatives
2. Outsiders (those individuals who do not have the authority to be on campus)
   a. Parents and relatives
   b. Former employees or students
   c. Visitors
   d. Students from other schools (such as athletic teams)
   e. Terrorists (gang members, foreigners making political statements, etc.)
   f. Psychotic individual
3. Other (severe weather or natural disaster)

Figure 2.2 Sample List of Undesirable Events and Threats in a School Environment

	Event: _____ _____	Extremely-Low	Low	Medium-Low	Medium	Medium-High	High	Extremely-High
	L Likelihood (Relative to other events; not a probability)	Virtually impossible	Rare, but not unthinkable	Can occur on occasion	Of average occurrence compared to other undesirable events	Likely to happen	Very likely to occur	Will always occur
CONSQUENCES	**COST** (Damage or losses sustained)	Less than $50	$50 to $1000	$1000 to $5,000	$5,000 to $10,000	$10,000 to $25,000	$25,000 to $100,000	Greater than $100,000 loss
	Bodily Injury Sustained	No injury sustained	Very minor injury(s) ustained	Injury is treatable by school nurse. Recuperation may require absence from school	Injury requires treatment by physician, absence from school	Injuries are serious with possible long-term or life-long effects. Hospitalization required.	Injuries are life threatening. Death could occur without immediate medical attention	Injury results in death or permanent incapacitation
	Disruption to Operations (Teaching and / or Learning)	Not disruptive to staff or students	Rarely would result in disruption	Occasionally causes disruption to classes	Exasperating to administration and degrading to school's Order Maintenance	Parents are involved and concerned; some student(s) run risk of flunking classes or not finishing school	Causes several students to drop out of school; good teachers leave to work at other schools	Many students fail to complete their schooling; school has a hard time hiring good teachers
	E Effectiveness -Security system's ability to prevent or mitigate undesir-able event; or apprehend instigator.	Useless	May be marginally effective	Occasionally effective	Of average effectiveness compared to other protection measures	Likely to prevent or interrupt undesirable event	Reliably effective without concern	Not possible for undesirable event to occur due to effectiveness of protection system

Figure 2.3 Sample Example Qualitative Measures of Likelihood, Consequence, and Protection System Effectiveness, for a Specific Undesirable Event

Assigning qualitative measures of consequence (C) to each pair may take a little more effort, because you may be concerned about more than one type of consequence. A single event might have several categories of consequence (such as dollar cost, degree of bodily injury sustained, amount of disruption to school operations, etc). Determine which consequence type(s) is most important to your school, and then assign a qualitative value *(Extremely-Low, Low, Medium-Low, Medium, Medium-High, High, and Extremely-High)* to each consequence category used, for each Undesirable Event/Threat pair. The example in the second, third, and fourth rows of Figure 2.3 shows three categories of consequences (Cost, Bodily Injury Sustained, and Disruption to Operations), with corresponding qualitative measures of the expected losses.

Develop one or more consequence categories depending on what consequence(s) are important to your school or district. If more than one category is used, use the maximum consequence value assigned within each Undesirable Event/Threat pair as the final consequence value in the rest of the analysis. For instance, suppose a particular event was assigned a cost consequence of *Extremely-Low*, a bodily injury of *Low*, and disruption to learning of *Medium*. The total consequence for this particular incident would be rated as *Medium*, the highest of the three. This method will allow different schools to rate the same undesirable event with different likelihood and consequence values. This is desirable because schools are unique in the likelihood and consequence of security risks they face.

Prioritize the Undesirable Event/Threat pairs

Once the relative measures of Likelihood (L) and Consequences (C) are identified, they are plotted to generate a qualitative grouping (also called a scatter plot) of these events. This helps decision makers to determine their ***priority undesirable events/threats***, or which are the most important to address first.

Figure 2.4a shows a sample form you might use to rate the likelihood and consequence of several example undesirable event / threat pairs. (Again, be sure to use one or more categories of consequence that are important to your school.) The pairs can be plotted using a chart similar to that provided in Figure 2.4b, where the x-axis is the measure of Likelihood (L) and the y-axis the measure of Consequence (C).

Events appearing in quadrant II have high Likelihood and Consequences and are of great concern. Measures should be taken to reduce the likelihood or consequence (or both) of these events, such that they move more toward the center of the graph, or even to another quadrant. Quadrant II points are called the ***priority undesirable events/threats***. Points in this quadrant require immediate attention. Events appearing in quadrant III (where both Likelihood and Consequence is low) are of low priority. Schools might attempt to address them, despite their lower priority, if it is inexpensive and easy to “fix” them.

Main Street H.S., Little Town, ST			Relative Likelihood	Relative Consequence (C) in Terms of:			Maximum Consequence
Pair	Undesirable Event	Threat	(L)	Cost	Injury	Disruption	Value (C)
A	Theft of school computer (nighttime)	Students					
B	False fire alarm pull	Students					
C	Drugs being sold on campus	Students					
D	Drugs being sold on campus	Gangs					
E	Alcohol consumption during lunch	Students					
F	Irate parent assaulting teacher	Parents					
G	Theft of student org money	Students					
H	Vandalism to vending machines	Students					
I	Hostage situation	Terrorist					
J	Shooting inside school	Students					
K	Students skipping classes	Students					
L	Graffiti	Students					
M	Graffiti	Gangs					
N	Bomb threat (false)	Students					
O	Bomb threat (real)	Psychotic					
P	Fighting on campus	Students					
Q	Fighting on campus	Gangs					
R	Robbery of cafeteria cash register	Students					

Figure 2.4a ***A sample list undesirable event / threat pairs. After likelihood and consequence values are assigned, they can be plot using the blank chart in Figure 2.4 B.***

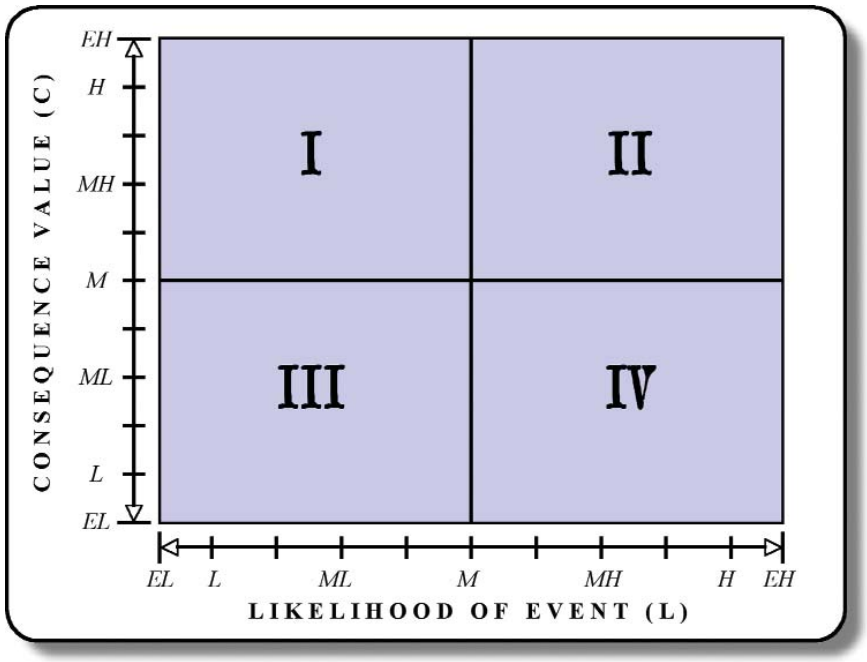
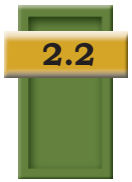


Figure 2.4b ***Use a chart similar to this to plot (L) versus (C). Breaking the plot into quadrants allows grouping and prioritization of the undesirable event / threat pairs.***

Quadrant I contains events that are relatively unlikely, but result in high consequences. Quadrant IV contains events that are highly likely (perhaps even occurring every day), but have very low consequences. Quadrants I and IV are definitely of concern, and it is here that administrators must make decisions as to what is more important to address and where to spend their resources. Risk management plays a key role in these quadrants, because there are many tradeoffs between performance, cost and risk. Additionally, it is difficult to know whether to first address the low-consequence, highly likely security incidents (quadrant IV) or the high-consequence but unlikely security incidents (quadrant I).

Whoever is ultimately responsible (the principal, district security manager, school board) for the safety of students, staff and school assets, should make the final prioritization of the Undesirable Event/Threat pairs. All the pairs could be chosen as "Priority" initially, but available funding will usually shorten this list quickly. It is important to not get too bogged down in the prioritization method just presented – the point is that the decision makers need to set priorities on what security incidents are the most important, using an assessment method that incorporates risk into the decision process.



2.2 Set Protection Objectives for the school's security system

Following the process described above results in a prioritized listing of credible security risks (undesirable event / threat pairs). We now must decide what to do about them. The recommended approach is presented in Figure 2.5.

For school stakeholders to feel that there is "enough security", an objective standard or measurement is needed that allows impartial judgment as to the system's effectiveness. The standard that is used in the security industry is referred to as a protection objective. Protection objectives provide the strategic basis for how a security system is designed – they define exactly what the system must do. If the protection objectives are not met, then the security system is judged to be inadequate.

Each Undesirable Event/Threat pair of concern must be assigned a protection objective. Each protection objective is composed of discrete **functions**. In general, the school's security system must successfully perform all the functions associated with the selected protection objective in order to meet the protection objectives. These functions occur through a combination of

- Manpower,
- Procedures,
- Security equipment, and/or
- Facility layout

Three protection objectives that are reasonable for use in school environments are: apprehend, prevent, and mitigate. The protection objective assigned to each event/threat pair should be based on what it is

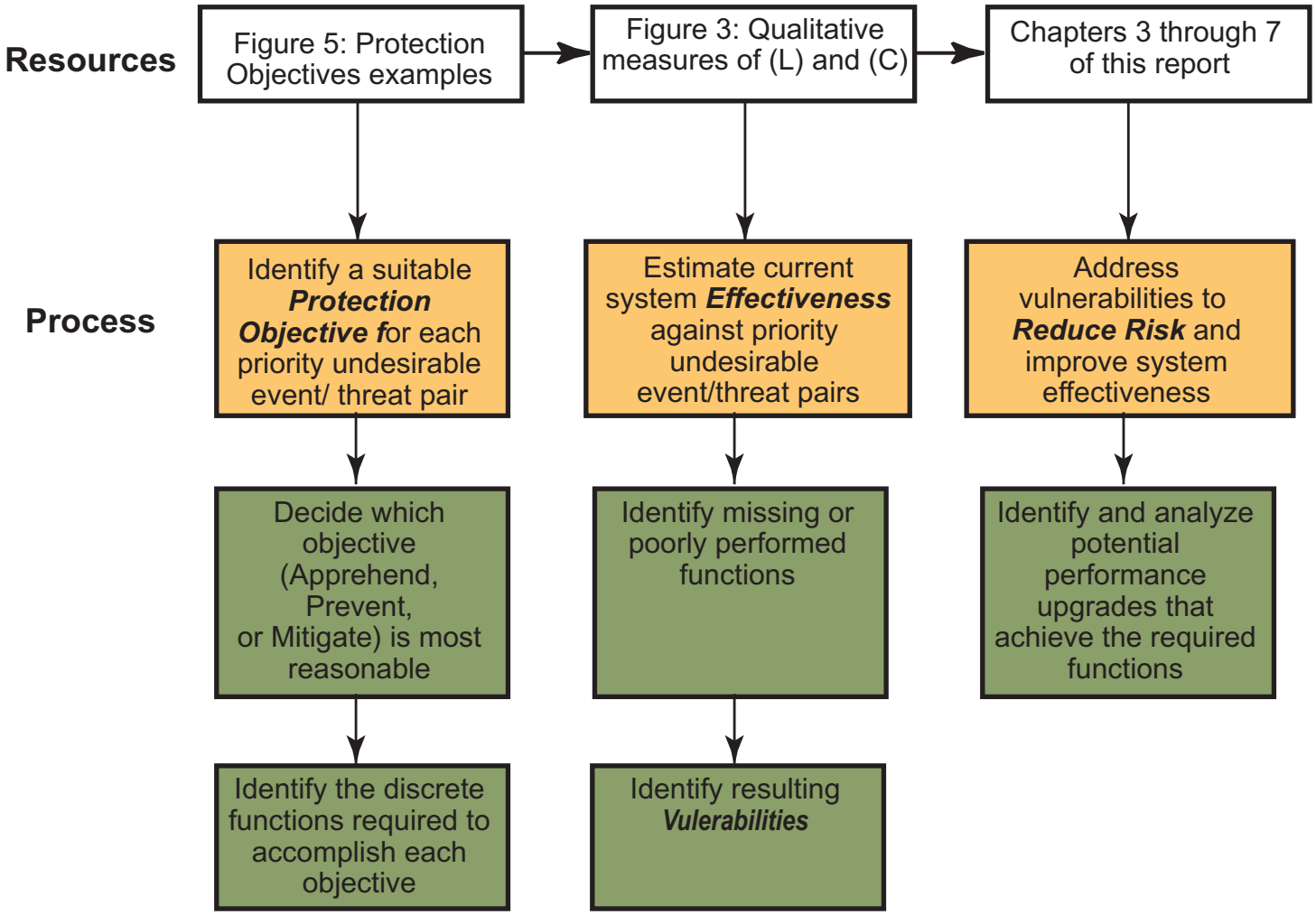


Figure 2.5 Recommended process for addressing vulnerabilities to reduce risk.

you want to achieve with respect to that problem. That is, do you intend to apprehend and prosecute the person after the fact, completely prevent the incident, or simply mitigate its consequences?

A word about deterrence

Principals would of course like to deter all possible security incidents from ever occurring. But how does a school go about achieving deterrence? How do schools convince potential adversaries to not attempt some undesirable event?

Deterrence is best achieved (against most people) when the school has an excellent reputation for security. That is, whenever a security incident does occur, the person is identified and punished due to the robustness and effectiveness of the school's security system in meeting its protection objectives.

If people believe that they will be caught if they attempt a particular undesirable event, and an unpleasant disciplinary action or prosecution is certain, most will likely decide against attempting the undesirable event, and the event has then been deterred. (The exceptions to this rule are people who are under the influence of alcohol or drugs, or who no longer care about consequences for their actions.)

This means that (1) the security system must have a HIGH likelihood that a person will be caught (and/or sufficient evidence will be collected to correctly identify that adversary) and, (2) there will definitely be unpleasant disciplinary action or even prosecution as a result. For example, if word gets around that a student will get caught if he brings drugs onto campus and will face severe disciplinary action, then eventually most students no longer consider bringing drugs to school. The bottom line is that deterrence is the natural result of consistently meeting the protection objective assigned to each undesirable event/threat pair.

The Apprehend Protection Objective

To accomplish the apprehend protection objective, the security system must effectively perform all of the following functions:

1. Detect that an Undesirable Event is occurring;
2. Communicate the detection information to the appropriate personnel;
3. Apprehend the suspect, or collect evidence sufficient to identify the perpetrator and apprehend at a later time (– note that the suspect may have already been successful in his or her task so the undesirable event may have already occurred); and
4. Prosecute and/or discipline to the full extent allowable as appropriate.

For example, the *apprehend* protection objective might be applied in the case of students drinking during the lunch hour. A teacher notices (detects) that a student returning from lunch is obviously

intoxicated. The teacher notifies (communicates) to the School Resource Officer who intercepts (apprehends) the student before afternoon class starts and administers a breath test (collects evidence). The student's parents are notified and the student is suspended (disciplined).

The Prevent Protection Objective

Employing the *prevent* protection objective implies that, with a high degree of confidence, the security system is rigorous enough to prevent an adversary from successfully completing a particular Undesirable Event. This might be difficult for a school to accomplish but important enough to strive for against some undesirable events. To prevent an undesirable event, the protection system must perform the following set of functions:

1. Detect that someone is attempting the undesirable event;
2. Communicate the detection information to the appropriate personnel;
3. Delay the suspect from completing the undesirable event until response can arrive;
4. Respond to and successfully interrupt the incident before the event is considered successful, so that the Undesirable Event is *prevented*.
5. Prosecute and/or discipline the perpetrator as appropriate.

For example, imagine that you want to prevent school computers from being stolen after normal hours. In order for this strategy to work, an effective intrusion alarm must detect a break-in at some point along the intruder's path to the computer lab. The intrusion alarm must then notify the police (or security guards, or both) that there has been a break-in at the school, and the location of the alarm. If the computer lab is a locked interior room with no window, the intruder will be delayed while trying to break through the inner room's upgraded lock. *(Note: Delay measures occurring after detection are meant to create enough time for the police to arrive before the adversary completes the task of stealing the computer. Delay measures occurring before the detection point, such as fences or locked doors tend to act as deterrents.)* Additionally, the computers have been secured to the desks with cables, forcing the intruder to remove or cut them, creating additional delay. The police respond in time to interrupt and prevent loss of the computers because of the lengthy delay required to successfully steal a computer.

Consider the effort that would be required to *prevent* student fights. To actually accomplish this, it would be necessary to prevent any student at any time from raising a fist and striking another student – an event that is over after just a few seconds. Is it possible to detect that an individual is getting upset and then delay him long enough so that security can respond and interrupt before the fight begins? Probably not. Harsh punishment for fighting could be established as a consequence associated with an *apprehend* protection objective, but it is not likely

that the security system can *prevent* a fight. Apprehending the students after the fact is probably a more realistic protection objective.

An alternative *prevention* approach to the set of functions above is to remove the opportunity. For example, if students frequently tag (vandalize) a statue in the courtyard, the school administration might consider getting rid of the statue. If students are breaking into nearby homes during their open-campus lunch, the open-campus privilege could be cancelled. Using this approach either eliminates the target of opportunity, or reduces its value to the attacker to a point that it no longer a security issue.

The Mitigate Protection Objective

In some cases it will not be reasonable or logical for schools to implement a *prevent* or *apprehend* protection objective. For instance, undesirable events like suicide attackers, bomb threats, drive-by shootings, terrorism, or catastrophic natural disasters are extremely rare, extremely hard to prevent, and hard to deter. Sometimes the best that a security system can do is *mitigate* the consequences of an event such that chaos, property losses, and injuries/deaths are minimized. The functions usually required to mitigate these extreme events are:

1. Notify the appropriate personnel that a crisis is in process
2. Assess the situation, if necessary
3. Initiate the appropriate emergency procedures to be carried out by the school's occupants. These actions need to be well known and understood by staff and students through regular training, and
4. Optimize response effectiveness – have all the information that might be needed by an emergency response team (police, SWAT team, EMS, etc.) available in an easy to use and understandable format. This includes detailed copies of the campus and building layout, knowledge of where cameras are located and how to access real-time and recorded data, etc.

For example, if a hostage situation develops in the cafeteria, a cafeteria worker could initiate a pre-installed, covert duress alarm at the cash register. The signal is directly dispatched (notify) to police and the front office. If possible, a staff member from the security team or front office might assess the situation to determine if this is a true crisis situation. The security team then transmits lock-down procedures via intercom to all classrooms (initiate emergency procedures). The responding police are met in the parking lot by pre-designated security team members familiar with the details of the incident, and can show the police exactly where the situation is occurring (optimize response effectiveness) via maps. The security team informs the police whether it is possible to remotely view the situation (via live camera recordings in the crisis

area), or listen in on the crisis area via intercom. This might help the police determine the most effective way to end the situation while minimizing injuries. Figure 2.6 shows protection objectives assigned to some of the Undesirable Events/Threats from Figure 2.2 and Figure 2.4, including some potential methods of accomplishing the functions in each sample protection objective.

2.3 Evaluate the Effectiveness of the current protection system, and address vulnerabilities to reduce risk

At this point, it is necessary to know how well the current system (including policies, procedures, installed security equipment, etc.) accomplishes the protection objectives. A baseline measurement of the effectiveness of the current system is needed before rational decisions regarding changes or upgrades can be made. This also allows a future comparison of the effectiveness of the improved system against the current system, so administrators will know if resources were spent wisely.

Using the information gathered in Section 2.1 (information used to characterize the school), evaluate the current security system's effectiveness toward meeting each specified protection objective, for each Undesirable Event/Threat pair. A recommended process for evaluating the effectiveness is explained below, using Figure 2.7 and Figure 2.8:

1. Using Figure 2.7, list all of the functions that will be required to meet the protection objective for each Undesirable Event/Threat pair.
2. List all the features/components/procedures that exist as part of the school's current protection system that support each of those functions.
3. Assign a qualitative effectiveness measurement to each function, using the suggested measures provided in the last row of Figure 2.3. If these features performed as they normally do, what is the overall effectiveness in accomplishing each function? Does the security team believe that the current features are sufficient and reliable? (Several features can contribute to a function on an infrequent basis. For example, a teacher passing in the hallway might detect if someone breaks into a locker. Often, these infrequent features may be the best a school has until more funding is available.)

   Use the information provided in Chapters 3 through 7 to determine the effectiveness of features such as video cameras, video recorders, intrusion sensors, metal detectors, entry control, ID badges and procedures etc. Do this by comparing the installation, operation, maintenance, training, and performance of these security features at your school relative to the ideal conditions recommended in Chapters 3 through 7. Considering all of these features together, how effective is your security in each of the required functions?
4. Assign an overall effectiveness rating for each protection objective equal to the lowest rating of its associated functions.

Item	Undesirable Event	Threat	Protection Objective	Required Functions	Some Potential Solutions for the Protection Objective Selected...
A	Robbery, drug sales at open lunch	Student	***Prevent***	Remove opportunity	Close the campus at lunch.
B	False fire alarm pull	Student	***Apprehend***	Detect	The sounding fire alarm serves as the detection and communication. The alarm must be assessed to determine if it was real or falsely pulled.
				Communicate	Encourage students with information to come forward.
				Apprehend	Cameras / recorders of sufficient resolution to identify puller.
				Prosecute	Discipline appropriately notify other students of video evidence.
E	Drug use on campus	Students	***Apprehend***	Detect	Drug sniffing dogs SRO uses drug detection equipment or testing.
				Apprehend	Prosecute as appropriate notify other students of consequences.
				Prosecute	Have SRO apprehend student based on evidence.
F	Irate parent assaulting teacher	Parent	***Mitigate***	Notify	Entry control procedures 24-hour appt. notice duress alarms
				Assess	Dispatch SRO to duress alarm; use video-taped conference rooms.
				Initiate procedures	Call police School nurse also responds to duress alarms
				Optimize Response	N/A
H	Theft during night	Student	***Prevent***	Detect	Cameras in rooms with valuable equipment sensors in rooms/hallways.
				Communicate	Alarm status dispatched to local police.
				Delay	Locked windows, pry resistant doors, computers bolted to desks.
				Respond	Local police or contract guards respond to alarm and arrest suspect.
				Prosecute	Prosecute apprehended suspect.
I	Hostage situation	Psychotic	***Mitigate***	Notify	Have front office or SROs enforce campus entry control procedures
				Assess	Use PA system, cameras, or SROs to assess situation.
				Initiate procedures	Call emergency responders initiate school lock-down procedures.
				Optimize Response	Provide responders with updated information, campus maps, etc.
L	Graffiti	Student	***Apprehend***	Detect	New grafitti is spotted on school wall.
				Communicate	N/A Perhaps student calls in tip to hotline?
				Apprehend	Review previous night's camera recordings of the area.
				Prosecute	Prosecute if possible, based on evidence, confessions.
N	Bomb threat (false)	Student	***Apprehend***	Detect	Caller ID Record all incoming telephone calls.
				Communicate	Turn over recording and evidence to police.
				Apprehend	Identify and apprehend suspect.

Figure 2.6 Some protection objectives have been assigned to selected undesirable event/threat pairs listed in Figures 2.2 and 2.4

Protection Objective: _____

Undesirable Event: _____

Threat (Adversary): _____

Functions:

Features of the existing security/protection system that support each function:

Estimate the effectiveness of each function based on existing features. Use the remaining chapters in this manual to determine strengths or weaknesses of your installed security technologies.

The ability of your security system to perform this protection objective is equal to the lowest rating of each of the functions above, which is: _____

Is this level of security acceptable (i.e., good enough)? ❑ **YES** ❑ **NO**

If 'YES', then this particular protection objective is complete.

If 'NO', then vulnerabilities should be examined (continue to Figure 2.8).

Figure 2.7 Use this form to record function performance for each protection objective assigned to each undesirable event / threat pair.

List the features or components of the lowest-rated function of the Protection Objective. Which ones are ineffective and in need of improvement? These represent vulnerabilities in the lowest-rated function.

Possible improvements and upgrades to consider:

Based on these new features, estimate the effectiveness of each function.

Is risk reduced by these changes? ❑ **YES** ❑ **NO**

Is this level of security acceptable (i.e., good enough)? ❑ **YES** ❑ **NO**

If 'YES', then this particular protection objective is complete.

If 'NO', then consider other solutions for vulnerabilities.

Figure 2.8 Use this form to document vulnerabilities and potential upgrades for the ineffective features of functions listed in Figure 7.

5. Determine if the overall effectiveness rating is acceptable. If it is, then the protection objective for that Undesirable Event/Threat is accomplished. If it is not acceptable, continue to Step #6.
6. Using Figure 2.8, record the security features that make up the lowest-rated function, and determine which are ineffective and in need of improvement. These areas may represent vulnerabilities in the system. Are any features completely missing? What improvements or additions to this function should be considered?
7. Repeat the process beginning with Step #3, using one or more proposed functional upgrades (improvements), until the functions (and protection objectives) are determined to be sufficiently effective. Use the information provided in Chapters 3 through 7 for ideas on functional upgrades.
8. The security team or other decision makers must review the proposed improvements, or "upgrades", for feasibility (constraints will include cost, impact on operations, political acceptability, campus layout, time required to implement, manpower requirements etc.).

A few examples are presented to illustrate this process using sample undesirable events/threats and protection objectives.

Example #1: Weapons on campus

Imagine that at Main Street High School, the principal and his security team have determined that "weapons on campus/student" is a priority Undesirable Event/Threat. They select an *apprehend* protection objective, which requires the following functions:

- The act of bringing or having a weapon on campus must be detected
- The detection must be communicated to appropriate personnel, if necessary
- The suspected student must be apprehended and the evidence collected, and
- The student must be disciplined or prosecuted

The existing security features at Main Street H.S. that contribute to these functions are:

Detect:

- On one random day of every week, weapon searches are conducted in the morning on random students using hand-held metal detectors. Backpacks are hand-searched for any type of contraband. About one out of every 30 students is searched (a total of about 65 searches for a student population of roughly 2,000).
- Campus Crime Stoppers is available for any student who wishes to anonymously report a crime such as weapons on campus.
- The school has a policy that any student who is late to class or is found wandering the halls without a valid pass may be searched (including his vehicle) for contraband.

Communicate

- During random metal detector searches, a security officer is usually doing the searches, so no type of communication is necessary.
- The secretary who listens each day to the anonymous Campus Crime Stopper tips contacts one of the School Resource Officers (SRO) by two-way radio.

Apprehend and Collect evidence

- Armed SROs confront and search the students when communication to do so is received, or if they are wandering the halls without a pass.

Prosecution/Discipline

- A "Zero-tolerance" policy is imposed for any type of gun possession; students are expelled for the remainder of the year, and are turned over to the city police for prosecution.
- Alternative school setting is available for students who have been in trouble.
- Parents and student are interviewed by a counselor and an assistant principal before the student is allowed back into a regular school setting.

The security team rates how well Main Street H.S. performs each of these functions using the qualitative effectiveness measures in Figure 2.3. The overall effectiveness will be rated only as high as the lowest effectiveness rating of all the required functions for this protection objective. The ratings assigned by the security team are discussed below.

Effectiveness of *Detection*: Upon examining the guidelines regarding the use of metal detection equipment (found in Chapter 5), the security team feels that the handheld metal detectors and procedures used are appropriate. However, they feel that the random morning search examines too few students to be effective. For example, most students can easily see if a line is forming at the main entryway. This tells them that "today is random search day", so a student with a weapon will either leave the campus at that time or leave the weapon in a vehicle. Therefore, only a portion of the weapons on campus are believed to be detected. The Campus Crime Stoppers program has not been overly successful so far, though its use is increasing. The policy to search tardy and wandering students has been the most profitable method of detection so far. It seems that these students are typically the more troubled students and are more likely to have a weapon. The security team rates the effectiveness of their detection function as Medium-Low: "Occasionally effective".

Effectiveness of *Communication*: The effectiveness of required communication of detections or phoned-in tips is rated as High: "Reliably effective without concern".

Effectiveness of *Apprehend and Collect Evidence*: The ability of the SROs or administrators to approach a student and disarm him has been successful, with no major problems. Training is offered by the school district and the police department on a regular basis for this type of task.

The security team decides to rate the effectiveness of their Apprehend and Collect Evidence function as High: "Reliably effective without concern".

Effectiveness of *Prosecution/Discipline*: This function of the protection objective has seemed to work fairly effectively. The only issue that the security team sees is that occasionally the principal will not turn a student over to the police if the student makes good grades and this is his first offense. The security team rates the effectiveness of their *Prosecution/Discipline* function as Medium-high.

Because the effectiveness of a protection objective can only be as high as its lowest-rated function, the effectiveness of *apprehend* for "weapons on campus / student" is rated the same as the *detection* function: Medium-Low. This is unacceptable since weapons are a large problem at Main Street H.S. The team recognizes that security is not balanced – that is, from a systems perspective, security is sufficient except when it comes to detection. The school is vulnerable to weapons entering campus undetected. Therefore, resources should be spent improving the effectiveness of the detection function.

The security team identifies 4 options for upgrading the detection function, and determines the new detection function effectiveness for each option as follows:

1. High: Start a complete metal detection program using 3 portal metal detectors, hand-scanners, and an x-ray machine for baggage. Screen all students every day.
2. Medium: Use random screenings every day with the existing hand-held detectors, instead of only once a week.
3. Medium: Encourage students more often to use the Campus Crime Stoppers hotline to report suspicious activities.
4. Medium-high: Hire 2 more SRO's to help monitor hallways and search individuals without passes.

Implementing one or more of these options might sufficiently improve detection, though the first would require further feasibility analysis (on items such as installed cost, how many additional SRO's are needed to staff the portals, throughput, and impact on tardiness, etc). The option(s) selected will depend on how serious the school board and administrators are about apprehending students who bring weapons onto campus, and what resources are available. Alternatively, if it is infeasible (due to cost, impact on operations, or other constraints) to sufficiently improve the detection function, the team could investigate a *mitigate* protection objective instead.

Upon examining the proposals and speaking with vendors, the district estimates that option 1 will cost approximately $50,000 for equipment and an additional $100,000 per year for the additional manpower necessary to operate the equipment. The morning class start times would need to be staggered, to prevent large queues (and tardy students) at the main entrance. Option 2 will

require hiring an additional SRO and training of several staff members to assist in the added workload. Option 3 has no dollar cost, though it does increase the responsibilities for one or more staff members.

Although the full metal detection program dramatically reduces the risk of weapons entering campus (by increasing detection effectiveness to *High*), the district tells the security team that it cannot afford such a program at this time, given other necessary security upgrades (see Example #2). There is additional worry that not enough staff will be available to prevent students from bypassing the metal detectors via other entryways. The team decides that option 2 disrupts the morning schedule too much, for only a slight gain in system effectiveness. They select options 3 and 4, increasing the overall protection objective effectiveness to Medium-High for this priority Undesirable Event / Threat pair.

Example #2: Nighttime break-ins at school

The principal and his security team have also determined "school break-ins and theft at night / student" to be a priority Undesirable Event/Threat. Multiple break-ins in the past year have resulted in a few stolen computers and expensive repairs. They select a *prevent* protection objective, which requires the following functions:

- Each break-in on campus must be *detected*;
- An alarm condition must be *communicated* to the appropriate personnel;
- The intruder must be *delayed* in his task of breaking in and stealing computers so that the response team can arrive in time to catch the perpetrator;
- The responders must *respond* to and *apprehend* the intruder; and
- The intruder must be *prosecuted* or *disciplined*.

Detection

- The exterior doors, main hallways, and all rooms containing over $10,000 worth of re-sellable equipment are alarmed. While windows are not alarmed, the team believes that most perpetrators who enter by a window will eventually step into a hallway and be detected.
- Neighbors around the school are visited by the security team each year and are asked to report any suspicious activity on the campus that occurs after 10:00pm.
- The lights in the parking lots are operated by a motion detector. If a detection occurs after 10:00pm, the surrounding lights illuminate for approximately five minutes.
- The school district pays a contract guard to patrol Main Street H.S. twice a night at random times after 10:00pm.

Communicate/notify

- The interior alarm system immediately sends a signal to the district dispatch office if an intruder is detected.

Delay

- The most attractive (re-sellable) equipment the school owns is its computers. All computer labs are interior rooms with upgraded deadbolts and no windows.
- All computers and monitors are secured to the desks they sit on with a ? inch computer security cable.

Respond/apprehend

- The district's police officers are well-trained in apprehending burglary suspects.
- On most weeknights, one of the district's two contract police officers can usually respond to an alarm in less than 20 minutes. There are two police officers on duty for the entire district of 35 schools, so a response to a Saturday night break-in (which is fairly typical) might not occur for as much as 90 minutes.

The security team rates how well Main Street H.S. performs each of these functions using the qualitative effectiveness measures in Figure 2.3. The ratings assigned by the security team are discussed below.

- Effectiveness of *Detection*: The alarm system has been reliable, though nuisance alarms are common (such as from posters falling off walls in hallways). On several occasions, the district police have been notified of trespassers before any alarms were tripped, thanks to some nosey neighbors who noticed parking lot lights switching on and off. The value of the contract guard company that patrols twice a night is questionable, although they have reported unlocked doors on two occasions. The security team rates the effectiveness of their detection component as medium-high: "Likely to prevent or interrupt undesirable event".
- Effectiveness of *Communicate/notify*: The alarm system has not yet failed to notify the district office when an alarm is triggered. The security team rates the effectiveness of their communicate/notify component as High: "Reliably effective without concern".
- Effectiveness of *delay*: Locating computer labs in interior rooms with upgraded deadbolts, and locking the computers to desks with cables, has allowed district police to arrive at the school before most intruders were able to remove a significant amount of equipment. On two occasions, an intruder was able to break in and cut the cables before police arrived. The security team rates the delay effectiveness as medium: "Of average effectiveness compared to other protection measures".
- Effectiveness of *Respond/apprehend*: While the district police seem well-trained in responding to burglaries, most of the burglaries have occurred on a Saturday night, when response times have been well over an hour. The security team decides to rate the Respond/apprehend effectiveness as Medium-Low: "Occasionally effective".

- Effectiveness of *Prosecute*: The district has been largely successful in prosecuting or disciplining those who have been caught breaking in. The team rates the effectiveness as High.

The overall effectiveness is only rated as high as the lowest rating of the component functions, so the effectiveness of the *prevent* protection objective for "nighttime break-in and theft / student" is Medium-Low. It is now easy to see that Main Street H.S. is vulnerable to nighttime theft due to long response times (particularly on Saturday nights). Of course, the team already suspected this was the main problem. However, the team now recognizes that, even if the response function is improved to "medium-high", the new system vulnerability (lowest rated function) will shift to the delay function, since its effectiveness is only *medium*. A complete solution is needed that improves both the *delay* and *respond* functions, such that the team is highly confident the system will prevent a successful "nighttime break-in and theft".

The principal and his security team identify 3 options for upgrading the response function, and 2 options for upgrading the *delay* function. They are listed below with the new effectiveness estimates:

Proposed upgrades to the response function:

1. High: Use the contract guards to patrol the campus full-time on Friday and Saturday nights only, from 10pm until 2am, instead of twice-randomly every night.
2. Medium-High: Allow a city police officer to live on campus in his mobile home. In exchange for reduced rent and utilities, he can respond to alarms on nights when the district police are understaffed.
3. Medium-High: install a speaker system that is tied to the alarm system. When an intrusion is detected, a pre-recorded message annunciates: "You have been detected trespassing on school property. Please leave the premises at once. Police have been dispatched to arrest you".

Proposed upgrades to the delay function:

4. High: Use specialty bolts (very hard to remove without specialty tools) to secure all computers with high resale values (a total of 35 computers), instead of cables.
5. High: Install upgraded pry-resistant doors and jambs on interior rooms with expensive equipment.

The district and the security team evaluate the proposals and determine that option 1 results in a 5% cost increase from what the district is already paying the contract guards. Option 2 was determined to be too fraught with difficulties – space was limited, and these types of arrangements do not always work out as well as desired. Further, the contract would need to be renegotiated occasionally to ensure the school was benefiting from the arrangement. Option 3 will cost less than $5,000 installed. However, its effectiveness depends greatly

on how intruders will respond to it, and whether knowing the police have been dispatched will deter them from completing their task. Option 4 will cost less than $2,000 (including bolts and installation), and Option 5 will cost roughly $10,500 (assuming 7 doors at $1,500 per installed door). Other factors, such as maintenance or impact on operations, are not of concern in the proposed upgrade options.

The district selects options 1, 3 and 4 as the functional upgrades to implement. Option 4 was selected over option 5 because the cost was much less, for roughly the same amount of delay. The function that now has the lowest effectiveness rating is detection: Medium-High. (However, implementing option 1 has probably increased the effectiveness of the detection function too.)

If for some reason, the above options were infeasible or estimated to be insufficient to effectively prevent nighttime break-ins and theft, an alternative choice is to investigate an apprehend protection objective. For example, the school could install video cameras in rooms with valuable equipment. The recorder and room lighting could be linked to the intrusion sensors, and high resolution recording could begin when an intrusion is detected. This might allow sufficient after-the-fact identification of the intruders to apprehend (and prosecute) them at a later time.

Another potential risk management option is to use a mitigate protection objective. For instance, the school might increase its insurance premium and coverage to include any expensive computer equipment, rather than spend the money on enhancing the detection and delay functions. This option makes no additional attempt at deterrence or effectiveness (other than what is already in place at Main Street H.S.). Instead, it accepts the risk that an occasional break-in will successfully result in theft of a computer, with partial recovery obtained through insurance.

Addressing vulnerabilities to reduce risk

The intent of steps one through eight in Section 2.3 is to help schools reduce risk by addressing vulnerabilities in security. The examples used above illustrate some key points in this process:

- Security should be balanced across the protection objective functions, because the total effectiveness against a particular undesirable event and threat is only as good as the lowest-rated function.
- A complete solution is needed because more than one function may be "vulnerable" (as in Example #2).
- An *apprehend* or *mitigate* strategy might be more appropriate if it is infeasible (with a high probability or degree of confidence) to completely *prevent* an undesirable event.
- Security measures under consideration should be systematically assessed according to their ability to perform the functions associated with the selected protection objective.

- There are usually many tradeoffs to be made between performance, cost, risk, acceptability, training and impact on operations. This is why the systems-based risk management approach described in this chapter has such wide benefit. Schools must decide which strategy, or protection objective is the most appropriate, and which reduces risk the most within the constraints.

Even if the problems and solutions are obvious beforehand (as might be the case in Example #2 with the long response times), following this approach results in repeatable, traceable, documented, and defendable security decisions. Additionally, this approach should be followed before purchasing any security technology – schools need to first define what it is they are trying to protect, from whom, and what specific functional improvements are needed accomplish these objectives.

Contingency planning

The last consideration for a complete and acceptable security/protection system is to develop plans that may be followed during a period of heightened risk conditions. This type of **contingency planning** will include temporary measures that are reasonable for the school to implement and enforce for short periods of time. During such times, the *effectiveness* of the security system would likely become much more important than the cost, political acceptability, or other constraints.

Examples of such temporary measures might include:

- Locking all exterior doors, such that building entry can only be accomplished through the main entry where a temporary officer will be located;
- Keeping all window blinds drawn at all times;
- Canceling some after-hours or extra-curricular school activities;
- Closing all sporting events to non-students;
- Prohibiting backpacks; or
- Closing off the sections of parking that are located closest to the school buildings.

Summary

This chapter has presented a risk-based security assessment method for schools. Once the prioritized security risks are known, an appropriate protection objective is selected. The existing system performance is then evaluated and rated against each undesirable event/threat. This systematic examination of security issues and risks reveals the functional security vulnerabilities and target areas for improvement. This process can be repeated with proposed improvements, until a sufficient estimated level of security (or risk) is achieved, helping school administrators make the best security decisions possible.

The remaining chapters of this document present some security technologies commonly used in many schools today. Each of these is discussed in detail

as to strengths, weaknesses, appropriate applications, expected maintenance requirements, operational impacts, etc. The remainder of this document should make it easier to select appropriate security technologies, once a school has identified the specific functional security improvements it needs.

References

1. Biringer, B.E., "A risk assessment methodology for physical security", SAND2000-1995C, p1-14.
2. Biringer, B.E., and Danneels, J.D., "Risk assessment methodology for protecting our critical physical infrastructures", SAND2000-3119C, p1-11.
3. Garcia, M.L. 2001. The Design and Evaluation of Physical Protection Systems. Boston: Butterworth-Heinemann.
4. Jaeger, C. D., "Security risk assessment methodology for communities (RAM-C)", SAND2003-4766C, p 1-4.
5. Jaeger, C.D., "Risk assessment methodology for chemical facilities", SAND2002-0401C, p 1-6.
6. Matalucci, R.V., "Risk assessment methodology for dams", SAND2002-0439C, p 1-24.

Chapter III
Video Surveillance and Recording Systems

Following the systems approach defined in Chapter 2 will reveal which areas or assets at a school necessitate protection by means of video surveillance. Video surveillance is an important feature in a school security system that allows the recording of evidence and aids in identifying offenders. In the authors' experience, it quickly enhances student and faculty peace of mind and attitude. Additionally, video cameras tend to promote a perception of safety and authority, which contribute to the overall order maintenance of a school. This chapter discusses the advantages and disadvantages of video surveillance, effective uses of video cameras, installation and maintenance, digital video recording systems, and legal considerations on surveillance.

3.1 Advantages and Disadvantages of Video Surveillance

The primary advantage of video surveillance or CCTV (closed circuit television) in schools is in the ability to review recordings after an incident has occurred. These recordings preserve strong evidence that is useful to administrators and to our legal system. Many schools reported to the author that when students are shown a recording of themselves in an illegal or unacceptable act – even if the recording's resolution is insufficient to use for prosecution purposes in a court of law – they usually admit to the incident. Video recordings are also useful when dealing with parents, who may deny their child's guilt despite credible testimony. Many administrators have discovered parents will quickly accept their child's involvement in an incident when shown a recording.

Another advantage is that video cameras may reduce some adult supervision requirements on school grounds. For example, if cameras are covering a large patio area where students congregate during breaks, adults who normally would be assigned to oversee that area may attend to other matters of concern. However, should an incident occur, a camera in this example can only capture evidence – it can not respond to or interrupt an incident in progress.

It should be noted that in the example above, cameras may deter some students (or even outsiders) from perpetrating an incident because they fear they will be caught on tape, just as they might be noticed by a supervising adult. But not everyone is deterred by this risk. Cameras do not prevent or interrupt incidents – they only permit the recording of evidence. Additionally, faces can be masked and poorly placed cameras can be circumvented. This is why deterrence is only a minor benefit, and not the objective of video surveillance, or any other security feature at a school.

Finally, video surveillance provides solid documentation in liability claims. This may occasionally work against the school, but in the authors' experience, most schools welcome the concrete evidence it provides in verifying student or staff testimony.

The following are some of the disadvantages of video surveillance:

1. Cameras can be stolen or vandalized if not properly located and installed.
2. Cameras require periodic maintenance.
3. If it becomes well-known where the cameras are located, and what they can and can not see, students may simply move misbehavior to a different part of campus.
4. Insiders with full access to or knowledge of the video system can circumvent it to their advantage.
5. Some communities or individuals will challenge the legality of cameras from a privacy perspective.

3.2 Effective uses of video cameras

This section provides guidance on effective applications of CCTV systems in schools. It also discusses situations appropriate for real-time monitoring, use of color versus black and white cameras, and when to use fixed versus pan-tilt-zoom cameras.

Video surveillance may be applied to any area (or target) identified by the process outlined in Chapter 2. Section 3.1 explained that cameras do not prevent or interrupt incidents, they only record incidents when used in conjunction with recording devices. Therefore, the most effective application is in recording scenes where after-the-fact assessment of an incident will yield sufficient information to identify and prosecute the offender. The following is a sample list of proper applications of using a video surveillance system.

1. who started a fight in the hallway, and which students were involved
2. who is smoking in the parking lot
3. who stole blank CDs out of the computer lab
4. who pulled the fire alarm
5. who wrote graffiti on the school doors
6. who is vandalizing school property (windows, equipment, computers, labs, etc)
7. who slashed tires in a teacher's parking lot
8. why a student or parent became violent in the lobby or principal's office, and what took place

Some of these may apply to your school if these are objectives you identified using Chapter 2. The above examples are assumed to occur during school hours, when lighting conditions are suitable for video surveillance. A camera may have little benefit, however, if your objective is to identify a nighttime thief in the band hall or computer lab. The scene may be too dark to identify the thief; or he may have covered his face.

Occasionally, an irate parent or student may threaten an employee. This can be discouraged if individuals see themselves being recorded on a video monitor, as depicted in Figure 3.1. In this instance, video surveillance is being used in the lobby of some administration offices. In the authors' experience, visible cameras tend to discourage undesirable behavior in many (but not all) people.

Schools may want to consider classroom installation of cameras and recorder enclosures ("black boxes") that are currently popular on school buses. In a pilot school in west Texas a few years ago, cameras were placed in the black box of a classroom when the teacher felt that a class was getting out of hand on a regular basis. Signs underneath each black box stated: "Attention: It should be assumed that both video and audio are being recorded within this classroom at all times." After a year of availability, teachers who used the black boxes reported to the author that they felt safer and that the boxes discouraged misbehavior. (The author strongly discourages the use of "dummy" cameras. A potential victim may be under the illusion that he or she is being monitored and that help will be forthcoming in the event of an attack; this may create extensive liability concerns in schools.)

Monitoring scenes in real-time

Each year, a great number of CCTV systems are bought in the United States with the intent to assign a guard to constantly monitor the live video feed. The hope of this arrangement is that the person watching the monitor will detect an incident occurring (or about to occur), and a response may be dispatched immediately to stop the incident. This is an unrealistic approach to security, particularly in school applications. "Longstanding studies have shown that humans are not good detectors, particularly over long time periods" (Garcia, 2001).

Multiple experiments and studies have clearly demonstrated that humans are very poor at detecting suspicious events on monitors, after only 30 to 60 minutes of constant watching, even when told what the event would be (Tickner and Poulton, 1973, Ware, Baker and Sheldon, 1964, and

Figure 3.1. ***Occasionally, an irate parent may threaten a school employee, but this can often be mitigated if the parent sees himself being recorded on a video monitor. Several school administrators where this approach has been implemented have found this type of set-up very reassuring in some instances. Additionally, school administrators should always strive to meet parents initially near other personnel until the mood of the visit can be determined as friendly and reasonable. It would also be a good idea to have key phrases that all personnel in the office know the true meaning : "Please bring us some coffee", for example, could really mean "Call security quickly!".***

Mackworth, 1961). Monitoring video screens is both boring and mesmerizing – there is no semi-engaging stimulus, such as when watching a television program. In general, constantly monitoring video in real time is ineffective and a poor use of school security staff (see Figure 3.2).

There are three special instances where real-time monitoring of the CCTV is practical and effective. The first is using real time monitoring to actively grant individuals passage through a particular locked door. In this case, the security person at or near the video monitor receives an alarm signal 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 on a door to allow the person access.

The second instance is when a certain incident is expected to occur at school during a finite time period. For example, if cars in a parking lot are frequently broken into during the noon hour, security staff could actively monitor video from the lot during this hour so that they may immediately assess an incident in progress and apprehend the suspect. This would be particularly appropriate if the suspect is not a member of the school because obtaining images of an unknown person AFTER the incident is of little value.

The third instance is in covert surveillance, in which temporary, hidden cameras are installed and monitored to record a brief, specific and expected event. For example, there may be times when unlawful events (drug use, vandalism, or theft) are believed to be occurring on campus. With cameras in plain view, it is clear to all where not to carry out such dealings. It may be beneficial to temporarily install a camera hidden from view of the suspects, in areas not already covered by the existing CCTV system, after consulting with legal counsel.

Color versus black-and-white cameras

In school settings, the objective of video recordings is generally to determine the identity of individuals involved in incidents occurring during the day. In the authors' experience, higher-resolution color cameras are more useful for daytime surveillance. Color recordings contain much more information about the scene, allowing such assessments as "the boy who broke the window had dark brown hair, a dark green jacket, and drove away in a light blue car". This information is then compared against similar characteristics of students or outsiders known to frequent the area. Often, when the suspected student is shown a recording of himself in an incident, he will confess even though there may not have been sufficient detail for a positive identification.

Though color cameras tend to have lower resolution than black-and-white cameras (about 18% less resolution), the ability to identify the color of hair, clothing, or vehicles is often more important than a more-detailed black and white image. One exception to this would be a camera applied in an interior room where any potential perpetrators will be close

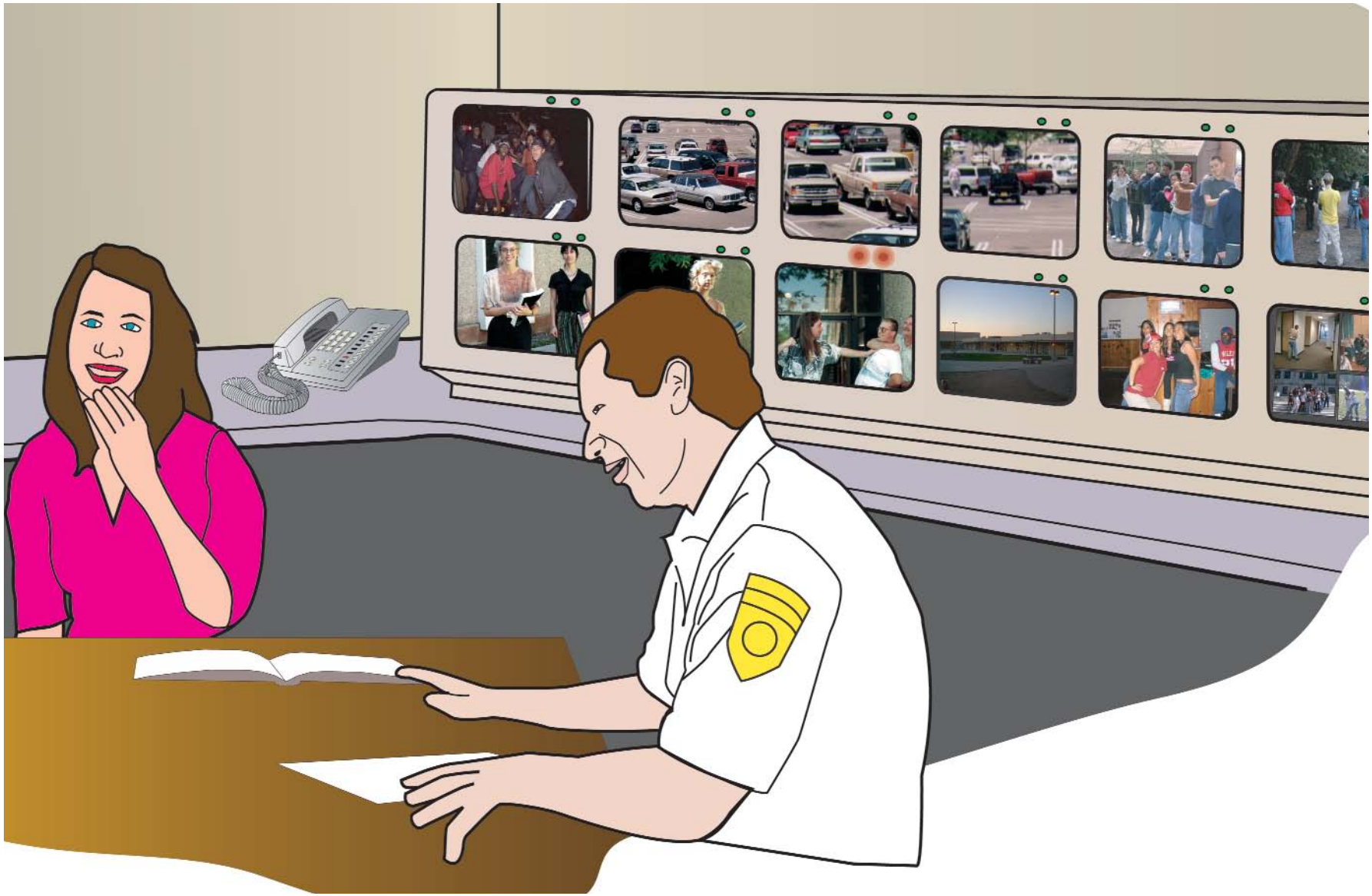


Figure 3.2 ***Monitoring video output is a boring task and usually non-productive in most security applications, even for the motivated employee. For this reason, using video recordings to determine what has happened in a particular incident after-the-fact is usually the best use of a school's resources.***

enough to easily identify them in black and white. Section 3.5 presents considerations for video evidence and resolution requirements when prosecuting in a court of law.

Finally, reduced light levels (such as in a parking lot at night with typical safety lighting) deteriorate the performance of cameras, especially for color cameras. Therefore it is necessary to evaluate the effectiveness of the existing lighting system to determine if it should be improved. A number of cameras on the market today are designed to operate in color mode during the day and in black-and-white at night. This is accomplished through software or an automatic mechanical adjustment.

Fixed versus pan-tilt-zoom cameras

Two popular types of camera configurations are 1) fixed and 2) PTZ (pan-tilt, or pan-tilt-zoom) cameras. Fixed cameras are mounted in a stationary position. These cameras will view the same scene until physically relocated or redirected. The scene is typically recorded, and in some instances might be viewed simultaneously on a monitor for brief periods.

PTZ cameras can operate in one of three modes. The most useful mode allows an operator sitting at a video monitor to physically change the direction and angle of the camera as desired using a joy stick type controller. PTZ cameras have a zoom option allowing the operator to focus more closely on parts of a scene, such as zooming in on a suspected perpetrator. In a second mode, the camera automatically scans either a predetermined or random path over a portion of its range. A third mode is to set the camera to act as a fixed camera, such that it continuously views the same scene. Normally a PTZ camera should be protected and shielded from view by an opaque enclosure (domes are most common) so that it is difficult for a would-be perpetrator to determine where the camera is actually aimed.

The author recommends using fixed cameras for most school security applications. PTZ cameras may cost ten times what an equal-quality fixed camera may cost and require a dedicated operator to operate the pant-tilt-zoom functions. If operated in automatic or random mode, the probability that the PTZ camera will be looking in the direction of an occurring incident (and capturing enough of that incident) is small compared to the probability that it will be looking in an unhelpful direction as in Figure 3.3. PTZ cameras require more regular maintenance (e.g., oiling gears, replacing motors, and cleaning the enclosure). Finally, a zoom lens requires higher lighting levels than a fixed focal length lens to achieve equivalent picture quality.

PTZ cameras can be effective when employed during specific portions of the day (such as the lunch period), if an operator is available to track suspects with the camera. Gateway High School in Denver, Colorado, has a dozen fixed cameras located throughout the campus but successfully uses one PTZ camera overseeing the parking lot, to watch

Figure 3.3 ***A pan-tilt-zoom camera that is set to automatically pan an area may completely miss capturing incidents of concern. For most school applications, the cheaper fixed camera is more appropriate.***

suspected perpetrators before and after classes. Gateway's objective for this PTZ camera is to obtain a recording of a suspected individual in a regularly occurring incident of which the school is already quite aware.

3.3 Design, installation and maintenance considerations

This section covers several aspects that directly influence the installation, cost, and operation of the surveillance system. These issues must be considered during the design of the security system and include wired versus wireless systems, camera housings, placement and mounting, lighting conditions, and use of covert cameras. The section concludes with a brief discussion on camera maintenance.

Wired versus wireless systems

Surveillance systems typically are wired with coaxial cabling that runs directly between the camera and the recording mechanism. Signal equalizers/amplifiers will be required to compensate for signal loss if cable distances become much greater than 1,000 feet (see Exhibits 3.4 and 3.5 for typical transmitting distances).

The author recommends that cabling for exterior cameras be placed within a watertight conduit. Above-ground cabling not protected by conduit is very susceptible to tampering and environmental degradation. Underground cabling should be buried below the frost line or at 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. With coaxial cable runs, ground loops (electrical currents 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. Surge protectors are recommended at both ends to protect equipment, because close lightning strikes can induce voltage surges on the cable that can damage equipment at either end.

Fiber optic cabling can be an excellent alternative to coaxial cable. Fiber optic systems are not susceptible to noise from RF (radio frequency) interference, ground loops, or voltage surges. However, fiber optic systems require a transmitter at the camera end and a receiver at the monitoring end. They require trained and experienced installers with specialized tools. They are more expensive than coaxial cable systems for short cable runs but become more cost effective at greater lengths (greater than 3,000 feet). Some schools have even successfully used their school network for signal transmissions.

Wireless systems are becoming more popular as the technology improves. These systems require a transmitter and power source at the camera, and a receiver at the video recorder. Acceptable distances between a transmitter and receiver may range up to

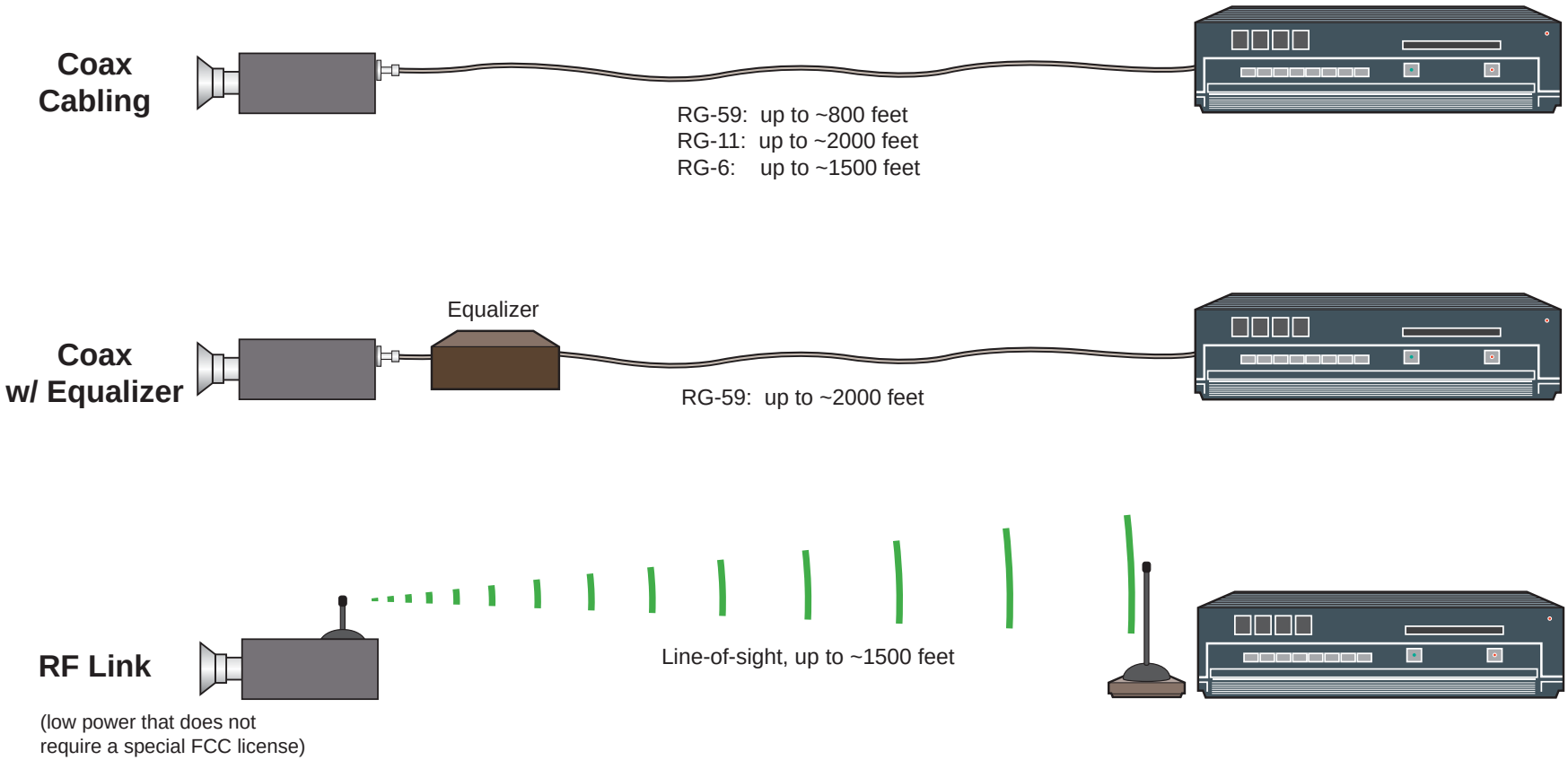


Figure 3.4 ***This diagram, along with Figure 3.5, illustrates typical maximum transmitting distances for hardwired and wireless camera systems. (Note: Some cameras have "pre-equalization" that will allow signals to go 1,000 feet farther than typical RG-59 signals.)***

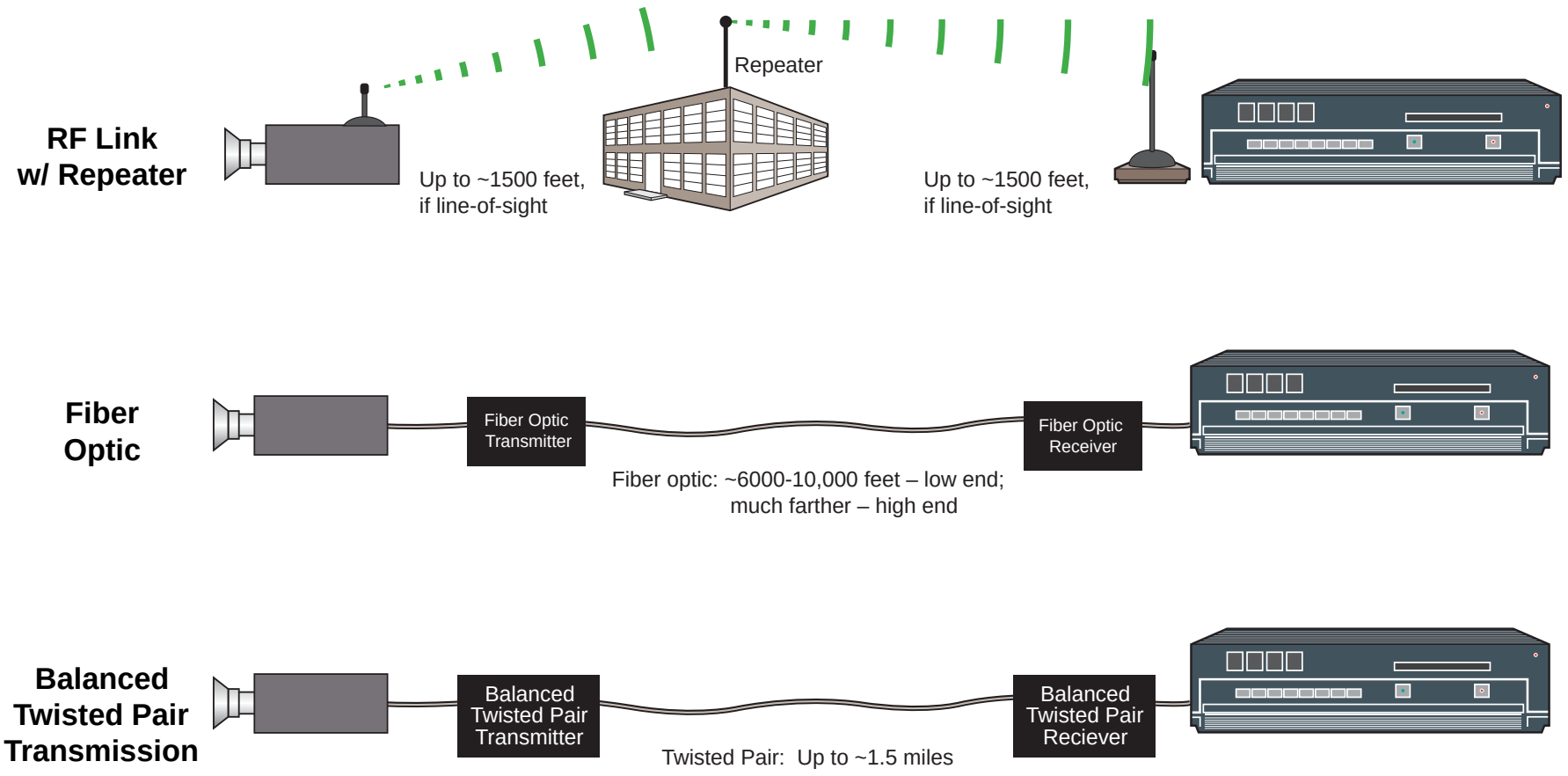


Figure 3.5 This is the continuation of Figure 3.4.

about 1,500 feet if the camera transmitter is in direct line-of-sight of the receiver.

One disadvantage of wireless systems is that inclement weather, transmissions through walls, fences, vehicles or trees, and exceeding the maximum recommended transmission distance degrades signal performance. The advantage of wireless systems is that protected cabling does not have to be run underground, through the air, behind walls or within ceilings (although cabling for power will still be needed). This also reduces the likelihood of cable tampering. Short-distance, low-power RF transmission systems usually do not require licensing by the FCC (Federal Communications Commission).

Camera housings

Camera housings can either help or hinder operation and maintenance. They protect the camera from the environment, reduce glare, prevent tampering and vandalism, and conceal (opaque dome-style) the camera's viewing position.

In the outdoors, a watertight housing is desired, and in some climates a heater may be required. Good ventilation is required in warmer climates. Some domed enclosures are a special version of housings that can be used to conceal the position of the camera. The dome housing may also offer a more attractive look that can be designed to blend into its environment. The key consideration here is that the housing should match the operating environment, which could be outside, inside, in a classroom, pool area, gymnasium, hallway, lobby area, etc.

A heater is recommended for exterior applications where the temperature will drop below 30 degrees F. Some auto-iris and zoom lenses can display mechanical problems at temperatures close to freezing (the lubricant gets thicker as it gets colder). A heater keeps lubricants warm and the lens and view plate (glass cover in front of the lens) free from condensation. In extremely cold environments (less than -30 ?F), it may be necessary to purchase a housing that is also insulated. *Specifications on operating temperatures should be included as part of the system design requirements, so proper cameras and housings are selected.* A sunshield is helpful in many environments because it provides artificial shade and reduces sunrise/sunset glare. It lowers the internal housing temperatures by 10-15 degrees F and provides a brim to protect the camera's view from direct snow and rain.

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.

If a camera is to be installed in a high-humidity, dirty or corrosive environment, a pressurized

environmental housing is recommended. A pressurized environmental housing prevents dust, humidity, and oxygen into the camera tube caused by changing atmospheric conditions, and will extend the life expectancy of a camera in these environments. Corrosion can be a major problem in areas near an ocean with high humidity and salinity, or near pools (chlorine is corrosive).

Smoke colored domes are important for camera installations in middle and high schools. Clear domes (see Figure 3.6) allow students to easily observe exactly which direction a camera is facing, allowing students to avoid detection. Additionally, there are reasonably good cameras available today in which the camera and lens are "bundled" into a custom housing with an appropriate mount. Some of these are turning out to be an excellent bargain for schools. Finally, upon examining their threat, some schools may require tamper-resistant or even bullet-resistant housings for their exterior cameras.

Camera placement and mounting

In an exterior application with a camera pointed 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. This will usually require a minimum mounting height of 18-20 feet. 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. Similarly, vehicle headlights and other sources of glaring light, particularly during night operations, should be considered. A correctly designed system will have identified and resolved these problems during the design phase – it may be costly and time-consuming to make design changes after installation.

Similarly, seasonal conditions should be anticipated and addressed before purchasing an exterior camera system. Some of these conditions may include: blowing snow, ice build-up on camera housings, dust storms, temperature extremes, dark building shadows which may affect scene assessment during winter months, and wind.

Cameras should always be mounted on solid surfaces to prevent as much wind movement and vibration as possible. Wooden poles may warp as they dry out, changing the camera view over time. If this occurs, the camera may require periodic scene re-alignment. Additionally, some slender (small diameter) metal poles vibrate in high winds, causing the auto-iris lens to constantly re-adjust. This makes the recorded scene unacceptably jerky. Newer equipment on the market can reduce some scene shaking in the recorded video through proprietary software.

The best way to prevent camera vandalism in schools is to locate the units where they cannot be reached without tall ladders or other equipment. Consider the height that would be required if a truck can be parked directly beneath the camera,

Figure 3.6 ***The vendor who installed cameras in this high school used clear domes, which allowed students to determine exactly which locations were being recorded. Because of that, this school saw little improvement in student behavior after the cameras went in.***

such that a perpetrator could stand on the truck's cab to reach the camera. A mounting height of about 18’ or higher is recommended.

Interior cameras cannot be mounted higher than the ceiling, making them susceptible to vandalism or tampering. Figure 3.5 (previously figure 3.17) shows an example of a camera installation that was immediately vandalized by students, even though the height of the cameras from the floor seemed more than adequate. This situation can be remedied by applying two or more cameras mounted at each end of a hallway or room, such that they are aimed to include a view of the other. This is referred to as “self protecting.” Similarly, most cabling should be enclosed in metal conduit (whether it is interior or exterior) for tamper protection.

Camera mounts should be rigid and secure enough that the camera does not vibrate under normal operating conditions. A mount designated for exterior use can be used for interior installations, but an interior 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). Mounts should have adjustable heads to allow adjustment of the camera field-of -view.

Lighting requirements and nighttime applications

Proper lighting is very important in exterior nighttime video applications because system performance quickly degrades without proper lighting. This section discusses lighting characteristics, including the type of lighting, illumination level, light-to-dark ratio, and lighting position. These issues are non-trivial and should be addressed by a lighting expert when designing the security system. (Note: Most schools will not use exterior surveillance cameras during the night, unless it is deemed necessary by the process in Chapter 2, because high light levels are required.)

If nighttime video surveillance is employed, lighting levels must be sufficient for the camera to produce a useable image. The level required depends on camera type, lens, sensitivity and quality. A systems approach is taught in this report for exactly this reason – performance is dependent on multiple interactions between system components. It is therefore incorrect to select or optimize one component of the system independently of the others.

Some common types of lighting are incandescent, fluorescent, and high-intensity discharge lights. Incandescent lighting is the most expensive (least efficient) to operate and includes the flood or quartz lights 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 (much more efficient) and is common in commercial applications, such as parking lots. This type includes high and low-pressure sodium lighting. Low-pressure sodium lighting is probably

Figure 3.7 ***While this camera installation in a high school's carpentry shop seemed plenty high, the fact that students could climb from the top of a table to the top of the lockers without being recorded by either camera and materials were available to use to beat at the cameras made this location easily vandalized. An additional camera installed to view the above scene would have provided a deterrence to prevent such an incident.***

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

Another type of lighting, known as IR (infrared), works with most black and white cameras (but not with color cameras) and is only slightly visible to the human eye. This is an advantage in situations where normally bright night lights would be inappropriate (i.e., for covert surveillance or in areas where bright lights would disturb nearby residents). Infrared light sources can be expensive to operate and maintain, and more light fixtures are required to illuminate an area than would be required with visible lighting. Some "bundled" cameras today come with their own IR lighting built in. In the authors' experience, the IR source in many of these cameras is only powerful enough to "light" an area no more than 20 or 30 feet away.

To make use of IR lighting, the camera must not have an IR cut filter. IR cut filters are routinely included within most cameras unless ordered specifically without. An IR cut filter gives better color rendition in color cameras. In black and white cameras, the IR cut filter helps reduce glare from IR sources in the scene being viewed. However, the IR cut filter will reduce or completely eliminate what can be seen at night if IR lighting is used.

Black-and-white cameras are generally more light-sensitive than color cameras and are recommended for all nighttime applications. A minimum illumination level of 1.0 foot-candles, as measured on a horizontal plane 1 foot off the ground, is recommended for a camera with a sensitivity specification of 0.007 foot-candles faceplate illumination. (This example illumination specification assumes the camera has a high-quality, F/1.4 fixed focal lens.) A color camera or a camera with a zoom lens will require greater lighting (1.5 foot-candles) in order to get equivalent brightness and contrast.

A recommended maximum light-to-dark ratio (maximum intensity to minimum intensity) for the lighting system 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 in the scene that a person or object would be obscured.

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

The lighting position relative to the camera field-of-view is also important. Light sources must not be visible in the camera's field-of-view, and lights used to illuminate a scene should be mounted higher than the camera. 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 scene, rendering portions of the field-of-view unusable.

Covert cameras

Cameras hidden from the view of suspects under investigation are referred to as covert cameras. There may be times when unlawful events (drug deals, fighting, intimidation, vandalism, or theft) are believed to be occurring on campus. With cameras in plain view, it is clear to all where not to carry out such dealings. It may be beneficial to temporarily install a camera hidden from view of the suspects, in areas not already covered by the existing system. Specific legal counsel should be obtained before installing covert cameras.

A whole new industry has arisen that specializes in these tiny (measuring only .5 to 1.25 inches square – see Figure 3.8), easily hidden cameras. Microphones are included with some cameras, but additional 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, etc., are available today. The lenses, including pinhole lenses, come in sizes ranging from 2.5mm to 25mm. Some covert kits provide both the camera and a set of lenses to handle a wide range of applications, including wide-angle and telephoto. Voltage requirements for covert cameras are normally 9 or 12 volts dc and can be provided by battery. In some instances, it may be practical to use a normal size camera if a convenient hidden location is available, such as behind an air duct.

One caveat is that the video recorder capturing the images must also be hidden from view. This may be difficult because the smallest video recorder is much larger than the smallest camera. It may require ventilation, a somewhat clean environment, accessibility, and it might make noise. It may be necessary to install the recorder in a separate secure room or even in another building. Additionally, the video signal must be transmitted either through cable or a wireless connection. In the authors' experience, wireless covert cameras may transmit up to distances of 300 feet, depending on the obstructions between the camera and recorder.

Maintenance and expected lifespan

After successful installation, the required regular maintenance of a fixed camera is to simply clean the lens and glass view plate on the housing. Occasional repositioning of the camera is needed to correct the viewing angle, especially for exterior applications.

Some camera housings come with wiper blades and a fluid dispenser. The dispenser mechanism is

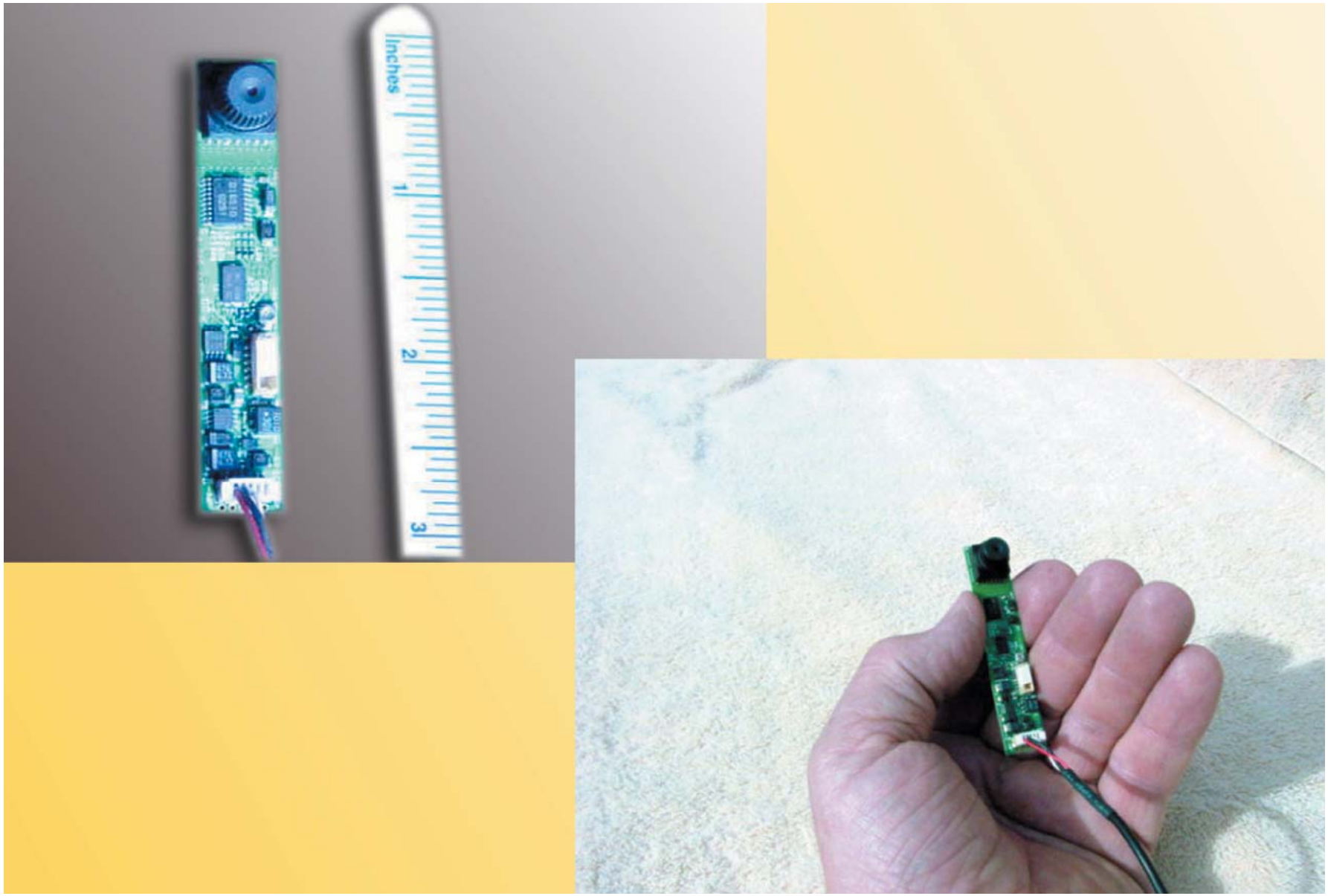


Figure 3.8 This photograph shows an example of the size of current covert camera technology.

activated remotely by an operator to keep the view plate clear. However, this feature can add to the required regular maintenance as the dispenser must be refilled with fluid. The mechanical wiper may also need to be replaced occasionally. Dust (or vandalism) can obscure the view of interior dome enclosures, but otherwise, maintenance is low.

The average lifespan of a modern solid-state camera is greater than 5 years, with high-quality cameras lasting over 25 years without replacement. However, recent declines in prices of sufficient-quality cameras may change the way schools maintain their surveillance systems. With some cameras available at $250 or less, maintenance is becoming a question of not "how to fix," but "whether to fix". Indeed, the cost of bringing in a lift just to reach a camera mounted advantageously out of any ladders' reach could well exceed the cost of the offending part. For a new 16-camera installation, stocking 4 extra cameras and vari-focal lenses may be easier than getting the vendor to find replacement parts and install them in a timely manner. Any electrician should be able to remove an old camera and install a new one. Aiming and focusing the new unit is then accomplished via radio communication with an operator at the recorder.

3.4 Digital Video Recording Systems

A recording system is necessary in order to capture the images from the cameras. This report recognizes that a few schools may be using VCRs (video cassette recorders) and multiplexers to record images onto analog VHS tapes. Though this is a viable technology, current digital video recording technology far surpasses the reliability and capabilities of VCRs, rendering them obsolete. Therefore, this report only discusses DVR systems. Readers who are interested in information on VCR and multiplexer systems should read the previous version of this report which is available from the National Institute of Justice.

In the author's estimation, no other product has made a bigger impact on the security market than the DVR (digital video recorder). A DVR is essentially personal computer (PC) with extremely large amounts of disk storage space (see Figure 3.9). It has very few moving parts which makes it much more robust than VCRs. Video images are stored in the DVR through specialized software that controls the video recording system. Some of the capabilities a school should request when shopping for a new DVR include the following:

1. The ability to view live video and to search or play back recordings while continuing to record current events
2. The ability to view single (full screen) and multiple camera outputs (see Figure 3.10)
3. Medium to high resolution when viewing images in real time
4. Medium resolution when viewing archived images
5. User-friendly operation
6. The ability to record only when scene motion is

Figure 3.9 The new digital video recorders (DVRs) are basically PC's (personal computers) that contain large amounts of disk storage and run customized software that directs and manages video images that feed into the DVR.

Figure 3.10 Most DVR systems will allow the user to view live video or pre-recorded video in a variety of screen arrangments. These photos show typical options of 16, 9, 4, or single-image displays.

present, to prevent storing enormous amounts of images unimportant to the user. (This is probably one of the best DVR features)
7. The ability to "mask-out" certain areas of a camera's view so the DVR does not initiate recording caused by motion unrelated to the school's security program
8. The capability to download saved video clips to a CD (compact disk)
9. The ability to access and view images remotely via a network or the world wide web

A typical 16-channel DVR takes up about the same amount of space as a PC. For a facility with multiple DVRs, the units should generally be installed in a metal rack designed to hold electronic components. Racks allow easier access to the units and keep most cables off the floor, as in Figure 3.11.

The author strongly recommends that a school's DVR and camera line terminations be protected in a locked room. In fact, the DVR should be part of the list of assets identified in Chapter 2 as needing protection. This is because the DVR is an excellent theft target, and video images (or evidence) will be irretrievable if a DVR is destroyed. Additionally, a convenient area is needed in which images may be viewed by authorized personnel, and this equipment is usually co-located with the DVR (see Figure 3.12).

Balancing image capture rate, resolution, and disk space

When all disk storage has been used to store recorded video images, the DVR rewrites over the oldest saved images. In this way, the most recent recordings are always available. While disk space is a factor, the number of days worth of recordings that can be saved before being rewritten also depends upon the number of frames (or images) captured per camera per second, and the resolution (or quality) of each frame.

When a scene contains motion, video should be recorded at a minimum of three frames-per-second. This usually preserves enough information to determine what has occurred in an incident. Two frames-per-second will not be sufficient for fast-moving incidents, like fights. Rates greater than six frames-per-second are much more pleasant to view, but are not necessarily more helpful in assessing a scene. Higher rates may be wasteful if storage space is very limited.

Most entry-level 16-channel DVRs record a total of 30 frames (or images) per second, which are then shared between the 16 (or fewer) cameras connected to the DVR. How these 30 frames per second are divided among the cameras is specified by the system administrator or according to default algorithms in the DVR (frames do not have to be divided equally amongst the cameras). The latest state-of-the-art DVRs can record up to 480 frames per second, or roughly 30 frames per second per camera, which is basically "real-time" video. However, just because greater frame rates are available does not warrant their use. Capturing more frames per second quickly consumes disk space.

The quality of an image generally refers to its resolution. The higher the resolution (assuming

Figure 3.11 This photo illustrates a typical installation of multiple DVRs within an electronics rack.

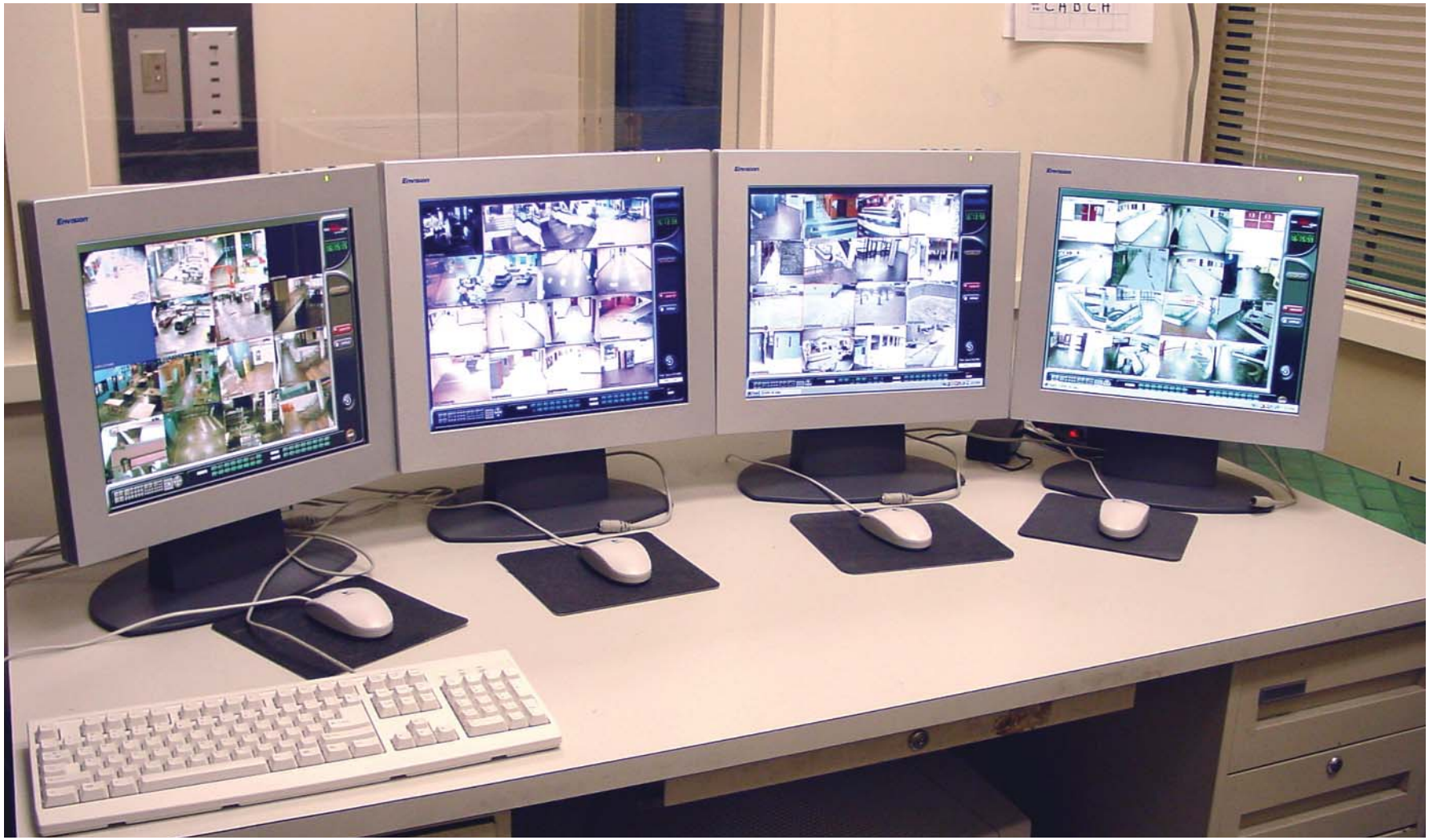


Figure 3.12 ***Shown here is a Boston school's monitor arrangement for its four DVR units. This equipment is located in an office usually kept locked but accessible by the school administration and security team. This particular brand of DVR does not require a keyboard after initial set-up is complete, only a mouse for each DVR's monitor. To simplify system changes, however, a single keyboard was installed with a four-way switch that then allows the user to alter camera view location names and other long-term changes. Note the difference between colors on the various monitors; as the DVRs were purchased at different times, the DVR manufacturer was installing a different video card at each of the various times, which created this discrepancy.***

image detail has not been lost in signal transmission), the more detailed and useful an image is in investigating an incident. For most school environments, a high quality image is very important, because the objective is to identify persons in a scene (i.e., which students were involved in a fight). A resolution of 640 x 240 is considered good quality; 640 x 480 is very good.

All DVRs perform a compression algorithm on each image before it is saved to in order to save days (or even weeks) of video images. When that image is to be played back, a decompression algorithm restores each image to a condition as close to the original as possible. Unfortunately, the algorithms of some DVRs can result in reduced quality. Many of these systems' algorithms can be modified to store higher quality images (see Figure 3.13). The author recommends that users examine several types of recorded scenes at varying resolutions to determine what resolution level is acceptable for their needs. Checking the specifications for decompressed image resolution will then help determine which manufacturer's units meet your resolution requirements.

In most school settings, saved recordings of the most recent seven days should be adequate, because most incidents are reported within a day or two (if not immediately). Several pilot schools within Sandia National Laboratories' school security program were generally able to save three to six days worth of good-quality recordings from 16 cameras onto a 120-Gigabyte disk. A 240-Gigabyte disk has usually held over a week's worth of recordings, using a frame rate of

Using multiple DVRs

Additional DVRs are required if the number of cameras exceeds the number of channels on the DVR. It is best to distribute the cameras evenly between multiple DVRs, so each will hold approximately the same number of days of stored images. Each unit will typically operate independently of other DVRs and have its own keyboard and mouse. This is an advantage because a portion of the system still works if one of the DVRs breaks down. Additionally, some camera cables can be reconnected to the spare channels in the working DVR.

When setting up multiple DVRs, it is helpful if the cameras assigned to each DVR are related in some way (i.e., DVR#1 records images for the 1st floor, DVR#2 is for the 2nd floor, and DVR#3 covers the gym and arts building). Further, a title can be assigned to each view to more easily identify the area. When accessing DVRs remotely via the web, each DVR should have its own unique address.

Cautions about web-accessible DVR images

Some vendors have painted a rosy picture regarding remotely accessing and monitoring images over the web. This requires the DVR to be connected to the school LAN (Local Area Network). Without a reliable, smoothly operating network, accessing your images will be problematic. Additionally, each remote user's

ability to view the images will be limited by the speed and bandwidth of the remote connection.

Making surveillance images web-accessible also creates privacy concerns. Internet hackers are skillful and persistent these days, and passwords are NOT enough to prevent illicit distribution of images captured by your surveillance system. Your images may be compromised unless very aggressive actions are taken by your network administrator (using software and hardware firewalls).

The author recommends that the system administrator establish a virtual priority for web-accessible surveillance video. For example, the security images may need to be guaranteed 20% of the total network bandwidth, regardless of what is going on in the remaining 80%. This is especially important if a hacker manages to set up a “doodle program”, which is an attempt to take over the entire system. If the system you are considering has web access, make certain the vendor addresses these concerns to your satisfaction. Better yet, ask the vendor to demonstrate web access using your video cameras and internet access provider.

Training

Most DVRs are user friendly, even for the occasional user who only wants to search for a particular incident. In the authors’ experience, about half a dozen people at each school, including school administrators and other appropriate security personnel, should be trained on using the DVR features. This type of training should take a maximum of 2 hours. Training for the DVR system administrator can be accomplished via the instruction manual over one or two days. It is helpful to send system administrators with minimal computer experience to a class offered by the DVR manufacturer or vendor.

Legal considerations

In the opinion of most legal scholars, the continuous video surveillance of public areas does not present significant legal obstacles. Under current interpretations of the First and Fourth Amendment and state tort law, silent video surveillance appears to represent a valid use of the state's power to protect its citizens. In this view, continuous video surveillance is analogous to a mechanical police officer. It does not intrude upon an individual's sphere of privacy, but rather records events occurring in public space for which individuals do not have reasonable expectations of privacy (Neito, 1997 and Sher, 1996).

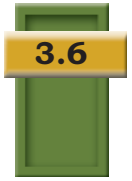
It is recommended however that administrators consult with their school attorney before beginning an electronic surveillance program. Additionally, requirements on video evidence necessary to prosecute suspects in a court of law should be known before selecting and installing a video surveillance system. Cameras generally 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).

Figure 3.13 These two images of a pre-recorded video scene illustrate the possible difference between different DVR vendors' compression and decompression algorithms in the quality and usability of an archived image.

Audio recordings are of far greater legal concern than silent video surveillance in most states, and present significant legal obstacles. This is because the recording of conversations is viewed as an invasion of privacy, as conversations often take place where the participants do not expect to be overheard. Accordingly, any video surveillance with an audio recording device must comply with Title I of the Electronic Communications Privacy Act of 1986 (18 U.S.C. Section 2510). A possible exception is to use clearly posted signs, in a specific room or area, which warns occupants that all audio and video is being recorded. Consult with your school attorney if audio recording is critical to the success of your security system, as determined by the process in Chapter 2.

Visible signs posted at major entrances to school buildings are an important legal consideration. Signs should state that video surveillance equipment is in use and that the equipment may or may not be monitored at any time. The purpose of this last phrase is to reduce liability. There have been cases where victims who were attacked did not try to defend against the perpetrator. The victim was under the impression that, because the attack happened in plain view of a video camera, it was being monitored and help would arrive soon. This is a common assumption and misconception. The victims filed lawsuits in some of these cases and won. The presence of video cameras should NOT lead a person to believe he or she will be rescued if attacked, because images are seldom monitored in real time (see Section 3.2). The author strongly discourages the use of dummy cameras for this same reason.

Signs are inexpensive, effective and their value to security should not be underestimated. In the authors' experience, signs that inform the public and school occupants that certain security measures are in force can provide a frontline deterrent. It is not necessary to post signs regarding every security detail being incorporated on a campus. It may be sufficient to insert a warning regarding the use of covert cameras into the school policy document, contracts signed by employees, and in contracts for outside services too.



Working with Vendors

In the authors' experience, security equipment suppliers, like those in other industries, will bid on and provide exactly what is asked for. In some cases standard options might be excluded by a bidder seeking to win the contract, if not specifically listed. If you can precisely describe what you require, the bidders will be less apt to submit bids on dissimilar systems.

If it is possible, have your purchasing agent word the RFQ and contract such that you will not accept or pay for the CCTV system until it has been installed and is demonstrated to operate according to your specifications. Acceptance criteria should be clearly stated early in the RFQ so there are no surprises for bidders. Acceptance criteria should include the "quality" of installation (see Figure 3.14). For example, a camera installer may try to save

Figure 3.14 This photo of a recent installation of exterior cameras on a high school campus shows two major installation mistakes; (1) cameras are installed too low and can be easily vandalized and (2) accessible wiring is not installed in conduit. A better solution for low cameras would be to use smaller bubble enclosures that are very difficult to grab once installed.

money by merely tacking cabling along the top of a wall instead of placing cabling within conduit in the ceiling.

Ideal specifications in an RFQ for a CCTV system will describe the desired performance criteria, rather than quantities of different components (such as number of cameras). For example, if it is desired to have cameras viewing locker areas to identify daytime thieves, do not request "two high-resolution cameras, installed at either end of the hallway." A more effective criterion might read:

> *"The CCTV and DVR system must be capable of recording at least three images per camera per second. The resolution of recorded and displayed images must allow an operator to distinguish between two similarly built and dressed individuals standing anywhere within the locker hallway. Quoted product and installation should be vandal-resistant, such that an un-masked individual can not disable cameras without being recorded and identified. The system will be tested upon installation by they client to the above acceptance criteria."*

Include maps, room dimensions and even a few photographs of the areas for which the equipment is intended, or require all potential bidders to view the area(s) before bidding.

In the authors' experience, it is common for bid prices based on performance criteria to be substantially higher than expected. The RFQ should therefore require bidders to submit two proposed designs and their associated costs. The first design layout would provide the exact capability and performance requested. The second layout might not meet all the criteria, but would be the best possible configuration within a specified dollar amount. The bidder should clearly identify the expected capabilities and deficiencies in this second layout. It is to both the school's and vendor's benefit to request these two different layouts — an administrator can approach the school board with this information to request the additional funding necessary to meet the performance objectives of the security system if the deficiencies of the less expensive, but more affordable system, are unacceptable.

It is common for defective cameras to fail quickly after installation. Someone should be assigned to regularly inspect equipment. Failing components should be removed immediately and returned to the manufacturer within the warranty period, or contact the vendor and make certain that he responds in a reasonable amount of time. If a camera unit used in a critical application must be sent away for repair, it is wise to have backup cameras available and stocked by the district. If a maintenance contract is used instead, the vendor should always address repair time and the availability of loaner units or spare parts.

The author recommends that, when selecting a DVR vendor, you obtain a brief list from multiple vendors of other nearby schools they have serviced. You should visit these schools and ask them to

demonstrate their system. Ask questions about the installation and operation of their DVR system such as:

- How helpful is the vendor / manufacturer when problems arise?
- What problems have occurred in the use of the DVR?
- What is the longest system down-time they have experienced?
- Did the DVR system administrator ever feel they had been abandoned by the company that sold them their DVR?
- How user friendly is the equipment and software?
- How many days of stored video does the school keep and what is the quality of the recorded images?
- How much manpower does it take to keep the system up and running?
- How useful has the DVR been for various kinds of security incidents?
- What would the school staff do differently in retrospect?

Similar questions can be asked regarding the installation and operation of their cameras and the vendor who supplied and installed them. Honest responses to these questions from other school's security personnel will provide the best information a new user can get.

References

1. Garcia, M.L. 2001. *The Design and Evaluation of Physical Protection Systems*. Boston: Butterworth-Heinemann.
2. Mackworth, N.H. "Researches on the Measurement of Human Performance." In Sinaiko, H.W., ed., *Selected Papers on Human Factors in the Design and Use of Control Systems.* New York: Dover, 1961; 174-131.
3. Neito, M., California Research Bureau, "Public Video Surveillance: Is It an Effective Crime Prevention Tool?" California State Library, CRB-97-005, June 1997.
4. Sher, S., Public Law Research Institute, "Continuous Video Surveillance and its Legal Consequences," University of California, Hastings College of Law, November 1996.
5. Tickner, A.H., and Poulton, E.C. "Monitoring Up to 16 Synthetic Television Pictures Showing a Great Deal of Movement" *Ergonomics* 1973; 16(4):381-401.
6. Ware, J.R., Baker, R.A., and Sheldon, R.W. "Effect of Increasing Signal Load on Detection Performance in a Vigilance Task" *Perceptual and Motor Skills* 1964; 18:105-106.

Chapter IV
Entry Control

Many school administrators reported ~~to the author~~ that the majority of their security problems and incidents were the result of unauthorized persons (people other than enrolled students and school staff) entering campus during school hours. Unauthorized persons are usually related to the school in some way. For example, trespassers might include suspended students, students from rival schools, irate parents, gang members ~~or~~ drug dealers with whom students associate. Measures can be taken to discourage and prevent unauthorized entry in schools.

An entry control system allows the movement of authorized personnel and material in and out of a school, while detecting movement of unauthorized personnel and contraband (Garcia, 2001). This chapter discusses entry control of personnel (~~and~~ Chapter 5 will discuss entry control of material through metal and contraband detection) and is intended to assist administrators that consider unauthorized entry a vulnerability at their school. The topics presented include limiting entry points, entry control methods, fencing, and identification badges.

4.1 Limiting the number of entry points

In the authors' experience, limiting the number of entrances onto campus and into buildings is the most effective way to reduce problems caused by unauthorized entry. In fact, none of the entry control methods presented in Section 4.2 can be implemented unless entry and exit points are first limited. Just as

with high security facilities, restricting normal entrance to only one or two locations greatly reduces the number of security personnel and 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 or the surrounding neighborhood. Many U.S. schools have been designed with open and inviting environments. Often, their layouts provide secluded niches; multiple buildings; multiple entrances and exits to maximize fire safety; and sprawling campuses. Without major remodeling for many schools, the manpower required to accomplish effective entry control can be enormous. Even some newer schools will often have over 100 exterior doors. Technologies such as card swipes and keypads can reduce this manpower requirement.

Deterring unauthorized entry

Many other measures can discourage and prevent unauthorized entry of casual intruders where it is impossible to eliminate an entry point. Some less technical but effective (as reported to the author by many administrators) approaches, are listed below.

1. Post signs warning that
   - 1.1. Unauthorized trespassers are subject to arrest
   - 1.2. All vehicles (including visitor vehicles) on campus are subject to search
   - 1.3. Vehicles parked on campus without a valid school sticker, other than in the designated and monitored visitor lot, will be towed
2. Institute and enforce policies for students that
   - 2.1. Require uniforms or standard attire for students. This makes outsiders easy to identify.
   - 2.2. Prohibit hats or headgear; saggy or baggy pants; t-shirts with alcohol, drug, violence, or gang affiliation messages for students. Again, this helps identify outsiders.
   - 2.3. Students walking around campus during class time will be challenged for a pass and/or student ID and are subject to being searched and scanned by a metal detector (to detect contraband).
   - 2.4. Expelled or suspended students will have their ID confiscated and (for larger schools) their picture made available to the security staff.
3. Have a guard check identifications at the main vehicle entrance gate.
4. Use greeters at all unlocked entrances into the school building (these can be parent volunteers).
5. Lock superfluous exterior doors to prevent entry from outside and label them inside to read: "For emergency exit only". Installing loud, local alarms or buzzers on these emergency exit doors will prevent most students from using them.
6. Make entry into the school during the day possible only through the front office.
7. Install fencing around campus that will

discourage the casual intruder and explicitly define school property boundaries.

Fencing

Fencing can effectively limit unauthorized entry onto school grounds. A robust fence defines property boundaries and forces intruders to consciously trespass. It also prevents idle wandering onto campus. The goal of fencing is to deter the casual or "unmotivated" trespasser. Administrators should understand that no fence will stop a determined and prepared (i.e., with a ladder or wire clippers) intruder.

Fencing does not have to be unattractive. Wrought iron fencing can enhance the appearance of some campuses while providing a difficult climbing barrier. An 8-foot chain link fence with small mesh (1-inch to 1-1/2-inch) can be an excellent barrier (it is difficult to climb an 8-foot high fence with mesh that prevents toeholds).

Fencing may be less useful for schools in remote locations. For example, if most students, staff and visitors arrive on buses or by cars, then simply restricting vehicle entry to guarded parking lots may be adequate. Also, fencing may not be beneficial if students do not normally congregate outside during the day.

Entry control methods

Once entrances are limited in number, verifying that someone is authorized to enter the school is generally accomplished through one of four methods. The first method is manpower intensive, and the remaining three employ technology devices. These entry control methods and their nicknames, in order of increasing security, are:

1. A security guard authorizes entry after verifying your identity. (Who lets you in)
2. A special ID card/badge/keyfob with automatic readers. (What you have).
3. A PIN number for entering on a keypad. (What you know)
4. A biometric device for feature recognition. (Who you are)

Method 1 is generally considered the least secure and easiest to implement, and method 4 is generally the most secure but hardest to implement. Each entry authorization method is discussed in more detail below.

Who lets you in

In this first method, a security guard or greeter at an entry point verifies whether persons wishing to enter are valid students, employees, or visitors. In smaller schools, the security guard is familiar with and simply recognizes persons requesting entry. Recognition is difficult in larger schools, so validation is accomplished through school ID cards (with photos) or badges, vehicle stickers, or mandatory school uniforms.

One guard located at a vehicle entrance can handle roughly 250-350 cars per hour, provided that

occupants are prepared to show ID immediately. A guard can handle between 300 and 800 people per hour at a personnel entrance, depending on whether the guard already recognizes most of the students, or if the guard must read each name, examine the photo, and match it with the person's face.

Although this is the most common entry control method, it not very secure for the reasons listed below, and is one of the more manpower intensive approaches. Schools studied by the author indicated that security guards cost between $8,000 and $40,000 per year (plus the cost of training and uniforms). An actual law enforcement officer can cost roughly two or three times as much. It is recommended that all members of a school's security organization have a thorough background check before being hired. Additionally, districts should require periodic drug testing for security personnel.

Sometimes a staff member can be assigned to this task after the morning rush, rather than employing a security guard for the entire day. A buzzer, camera, and intercom system can be located at an entry door. When a visitor arrives and presses a buzzer, this staff member receives a signal to check a monitor on their desk that displays the view of the person through a video camera. The staff member can speak with the visitor via the intercom and then open the locked door using a remote door release switch (see Figure 4.1).

Some strengths of this authorization method are:

1. In addition to checking an ID card, a security guard might perceive whether a student is drunk, fearful or acting abnormal.
2. A security guard can prevent two or more students from entering using one ID card.

Some weaknesses of this authorization method are:

1. A security guard in this task can become bored and desensitized.
2. A security guard's attention can be easily diverted.
3. A dishonest security person could allow unauthorized individuals to enter.
4. Using a person for entry control is an ongoing expense for the school.
5. Picture ID cards can be stolen and used by someone else. Experience has shown that security guards occasionally fail to notice someone using another person's ID card.

What you have

In this second approach, entry authorization is granted if proper credentials are presented. For example, a school-issued ID badge can grant access via a card-swipe reader or keyfob (see Figure 4.2). Validation of the card might electronically open a door lock, allow a turnstile to operate, or lift a mechanical arm extending across a parking lot

Figure 4.1 ***This illustration shows how a remote entry system could operate. During the school day students or visitors would be required to show ID or be recognized via the camera view in order for an operator to release the electronic door lock.***

Figure 4.2 Shown here is a teacher using a keyfob which releases the electronic door lock to allow authorized entry.

entrance. Viable card technologies for schools include

1. Cards encoded with a bar code or magnetic strip and used with card-swipe readers
2. Passive or active RF (radio frequency) cards used with proximity readers, which can validate a card up to several feet away (depending on the system).

Card-swipe readers are somewhat susceptible to vandalism as their read heads are fairly delicate. Proximity readers can be protected behind a solid piece of Plexiglas because actual contact with the card is not required. A proximity card reader might be an ideal entry control system for a teacher's parking lot, for an employee entrance to a building, or for a computer lab.

Some strengths of this authorization method are:

1. No operational manpower is involved
2. These are mature, stable technologies
3. Validation of a card can be turned off if a card is lost or stolen
4. An attendance database can be automatically updated when an ID card is read
5. The cards are generally tamperproof and most are difficult to counterfeit

Some weaknesses of this authorization method are:

1. Inability to ascertain if only one authorized person is entering an electronically activated lock per swipe or proximity read
2. Cards might be lent out and used by others without the administration’s knowledge
3. Card-swipe readers are subject to vandalism
4. Regular updating of the system database (who is authorized) is mandatory
5. Special arrangements are necessary for students who forget or lose their card

A high-quality, tamper-resistant encoding system (a printer, a digital camera, and software) more than adequate for most school's needs can be purchased for $3,000-$8,000. The electronic door locks, electrical panel, and computer system necessary to support a modest number of readers (typically at eight or fewer entry points) will cost about $2,000-$3,000. Installation costs may range from $500 to $1000 per door.

What you know

In this third approach, entry authorization is granted based on what you possess (usually an ID card) and what you know (usually a PIN). A confidential PIN (personal identification number) is entered after swiping the ID card and is compared to the PIN associated with that card. Although a PIN is easily compromised by onlookers, this is substantially more secure than using either a PIN or badge alone.

PIN-only systems (without ID cards) are secure when there is a relatively small population size that does not change often. A good example might be the locked chemistry storage room where only the

chemistry teachers know the PIN. 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.

The strengths of this authorization method are:

1. The PIN and associated ID card can be disabled by a system administrator as needed
2. An intruder can not gain entry with a stolen card because the PIN must also be known
3. It is possible to automatically update an attendance database when an ID card is read and the PIN entered
4. When used in conjunction with a floor-to-ceiling turnstile, an authorized person cannot bring in unauthorized persons (see Figure 4.3).

The weaknesses of this authorization method are:

1. More administrative effort is required to maintain a card and PIN system
2. It is possible for an authorized person to allow unauthorized persons entry along with him/herself (unless used in conjunction with floor-to-ceiling turnstiles)
3. Users can forget their PINs
4. Users can lend out their PINs and cards
5. Keypads are vulnerable to mechanical malfunction and vandalism

Who you are

In this fourth approach, a biometric device verifies the identity of a person through a unique personal attribute, such as hand or finger shape, fingerprint, voiceprint, signature dynamics, retinal pattern or iris pattern (Figure 4.4). Biometric devices are accurate and commonly used in high-security applications where unauthorized access into a facility is unacceptable. 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.

Many Biometric technologies use error rates as a performance indicator of the system. A Type I error, or “false reject”, is the improper rejection of a valid user. A Type II error, or a “false accept”, is the improper acceptance of an unauthorized person. Testing of hand geometry systems at Sandia National Laboratories indicates that Type I and Type II error rates of less than 1% are achievable (Holmes, Wright, and Maxwell, 1991). However, biometric devices cannot minimize both error types simultaneously. Administrators must decide based on objectives and acceptable risks, whether they desire more convenience (higher Type II error rates) or security (higher Type I error rates) (Garcia, 2001).

Biometric devices based on hand or finger geometry appear to be the most viable, affordable, and user friendly biometric system for school applications. Recently, two elementary schools in New Mexico have been using hand geometry systems to verify custodial parents. Abduction of a child by a non-custodial

Figure 4.3 ***Floor-to-ceiling turnstiles can regulate "tailgating". Without undue body squashing, only one person can enter through the turnstile upon approval of the magnetic car badge.***

Figure 4.4 ***Biometric devices, such as those depicted above, verify the identity of a person through some personal attribute. This type of identification is extremely accurate but may not be appropriate for many schools.***

parent is one of their greatest concerns and vulnerabilities.

Biometric technology is constantly improving and prices for most of these devices have stabilized. A single, stand-alone unit can cost between $50 and $5,000. A system that oversees and monitors biometric units at several doors can cost between $10,000 and $50,000 with installation.

Some strengths of this authorization method are:

1. Biometric identification is accurate and cannot be lent to other people, lost, or stolen
2. A user's identification can be deleted from the database when no longer appropriate
3. There is nothing for a user to forget to bring such as a PIN or card

Some weaknesses of this authorization method are:

1. It usually takes longer to use a biometric device than a card reader or keypad
2. The devices are subject to damage from vandalism
3. Some devices cannot be used by persons with physical handicaps
4. Except when used with a floor-to-ceiling turnstile, it is possible for an authorized person to let in an unauthorized person
5. Some of these technologies are not completely mature (such as voice recognition) and occasionally reject an authorized person
6. Most biometric devices must be sheltered if used outside

4.3 Identification badges in Schools

A significant portion of large high schools today are considering, or have already implemented the use of identification badges. Some benefits of badges are that they:

1. Identify students and non-students, permanent, temporary or district staff, parents and outsiders for the purposes of entry control (see Figure 4.5)
2. Automatically insert student ID numbers encoded on the badge when using library or cafeteria services
3. Allow a card or proximity reader to open electronically locked and operated doors
4. Identify students in detention, Saturday-school programs, and at mandatory tests
5. Allow visiting parents to address teachers or staff members by name
6. Admit students into after-school functions, such as dances or games
7. Validate identity and grade level for the issuance of parking permits that only juniors and seniors may have
8. Validate identity for issuing of refunds and grade cards, picking up ordered materials, or new class schedules

Figure 4.5 ***One excellent use of ID badges is for entry control. An administrator or security person is located at every unlocked door before school starts, where they can check to make certain that every student entering the building has an appropriate ID. The major problem with this type of entry control is the amount of manpower that must be dedicated to it.***

9. Validate identity for special upper-class perks, such as going off campus for lunch or leaving early for work-study programs, etc.
10. Help teachers address students by name

The last reason listed is probably the most important – to eliminate the anonymity of students in larger schools. In the authors' experience, students naturally show more respect to an adult who can address them by name, and this makes interactions between staff and students more personal. Students are less likely to be rude or ignore a staff member, because the student can be reported and dealt with later. And if the student is not wearing a badge, security should be contacted immediately, as he/she may not even be a student at this school.

Schools with smaller student populations might see fewer benefits from using ID badges. Some principals and security officials reported to the author that anonymity was a problem once the population reached 800 students. Others felt they knew and recognized each of their students up to a population of 1500. Certainly school populations exceeding 2000 should incorporate an identification system, just as businesses or government organizations this large would. Administrators must determine if ID badges will help accomplish their security objectives based on the unique characteristics of their schools.

An ID badge policy can initially be difficult to implement. Roughly 90% of the students will conform and wear their badges. The remaining 10% can be extremely challenging as problems with students can easily consume the entire attention of an administrator every morning. Additionally, some staff members can be more reluctant to wear a badge than the students. Administrators and security staff must never fail to challenge and confront a student or staff member not wearing their badge. In the authors' experience, this is the most effective way to get students and staff to wear their badges.

In a 1999 project sponsored by the National Institute of Justice (NIJ), badges were used at a large high school to track tardy students (among other items). When the tardy bell rang, all teachers locked their doors. Staff and security personnel swept all tardy students still in the hallways to the office, where each student's barcode was scanned. A high-speed printer automatically printed a sheet for each student that listed the cumulative number of tardies. This sheet was also their pass to get back into their classroom. The computer program automatically assigned students with 8 or more tardies to Saturday or after-school detention. On the 6th tardy, the system automatically generated a letter addressed to the student's parent(s). The letter stated that their child would be disciplined upon the eighth tardy, and that the parent(s) would be responsible for transportation to and from the detention program. Contact the author if your school would like a free copy of this software program (written in FORTRAN).

Guidelines on using and issuing student ID badges

Students should be encouraged to come to school in the week before a new school year starts to have their photograph taken and ID badges issued. Once the students have their ID, they may register for classes, get their class schedule, check out textbooks and apply for a parking permit. Scanning a bar code or magnetic stripe on the back of the badge can automatically record and document these transactions, if this type of system is used.

The two most important items on a student ID badge are the student's photo and name. The photo should take up as much as one-half of the badge, and names should be printed in a readable, 18-point or larger, bold font. A narrow version of that font should be available for long names. The school or district name and logo are less important, and if used, should occupy as little room as possible on the badge (see Figure 4.6). A small space on each badge can be filled in with a special symbol or color if a student is enrolled in a work-study program and will be leaving during the school day.

A pre-printed design on the back of the badges can identify a student's grade level. For example, at one Texas high school which only taught grades 10-12, 9th graders who were sent to the high school because they were too old to be in a junior school any longer received a pink badge labeled "freshman" on the back. Many of these students became seriously motivated to finish their 9th grade requirements so they could receive their green "sophomore" badge.

Students should be issued a standard, free-of-charge lanyard, which must be worn around the neck with the ID badge properly attached to it. Special or fancy lanyards can be sold to students for student fund-raising purposes. It is important that only these school-sanctioned lanyards be allowed on campus, to prevent inappropriate colors (such as local gang colors) or graphics.

Many school administrators feel that it is important to order "break-away" lanyards to prevent a student from being choked with his own lanyard. However, as the break-away part of a lanyard is usually located at the back of the neck, it is still possible to grab the lanyard from the back and inflict harm.

The author recommends that once school starts, students, staff and visitors should not be allowed to enter the school without appropriate badging (see the next section – Forgotten, Lost, Temporary, and Visitor Badges). Additionally, students should not be allowed to attend school functions without proper ID.

Forgotten, lost, temporary, and visitor badges

Forgotten badges are one of the more difficult aspects of implementing a badging program. If generic laminated passes are used in these situations, they must be collected at the end of the day to prevent students from keeping and passing them to others. This is nearly impossible in a school environment. A better solution is to issue a temporary badge that expires at the end of the day.

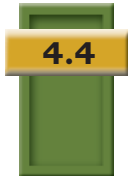

Madison H.S.
James Smith
"Excellence in Education"
2004 - 2005
Madison High School
James Smith
2004 - 2005
Emergency Codes & Pro
Code Red (or 1 long whistle) -
Proceed to nearest room w/ a lo
behind furniture away from all v
Code Blue (or repeated 3 whis
Weather Alert - Move away from
to inner classrooms & basemer
Code Yellow (or repeated lon
whistles) - Stay where you are,
further instructions.
Emergency Phone #s
Mr. Bellerty 656-3122
Ms. Tolsty 656-3157
Mr. Wethington 656-3195
School Hours:
7:25am to 3:10pm
A Lunch - 11:20 - 11:45
B Lunch - 11:50 - 12:15
C Lunch - 12:20 - 12:45
Class Schedule:
Period:
1: Science, Prince, 331
2: English, Samson, 171
3: Algebra II, Hillington, 146
4: Homeroom/Lunch, Jersey, 331
5: PE, Johnson, Gym
6: World History, Barnes, 348
7 42709 10018 5
Senior
Junior
Sophomore
Freshman

Figure 4.6

In the 1999 NIJ-sponsored project mentioned above, students who had forgotten their badges were issued a "self-expiring", stick-on badge (for which students were charged $1.00). This type of badge contains a safe chemical that causes red stripes and the word "EXPIRED" to appear after approximately 24 hours (see Figure 4.7), preventing inappropriate reuse. The badges cost about 25¢ each. Some schools use self-expiring badges that are custom colored – yellow for visitors, pink for substitute teachers, and blue for the forgotten badges. One unexpected but very positive outcome of the pilot project was that proceeds from the temporary badges totaled nearly ten thousand dollars. However, this school was located in a slightly above-average socio-economic area, where most students did not have a problem paying the $1.00 fee.

If plain peel-and-stick paper badges are used instead of self-expiring badges, the expiration date should be written in large print with a brightly-colored marker. The color of marker and/or sticker should probably be rotated daily, to prevent counterfeiting. Peel-and-stick paper badges are highly recommended for visitors as well.

A new badge must be issued if a student loses a permanent ID badge. One reasonable approach is that the first replacement badge is free, the second replacement costs $5.00, but for the third replacement, the student's parents must come in with the student. Regardless of how lost or forgotten badges are handled, discretion is needed with repeat offenders. Some forms of punishment for losing (or forgetting) a badge may cause a student to simply skip school rather than face the consequences.



Working with the vendor

Identification cards and readers are the most practical technology for schools needing a technology based (manpower-free) method of entry control. (Biometric devices might be necessary in some cases, though the enrollment of thousands of individuals in a biometric database can take several weeks.) A wide variety of card styles and features are readily available from vendors. Trade shows, such as the annual ASIS International seminar, can familiarize school security personnel with products available on the market. Some good questions to ask a vendor are:

1. What is the cost of the basic printer, digital camera, and software? What additional upgrades are available, what do they cost, and what additional benefits do they provide?
2. What are the minimum requirements for the computer running the system? How fast are cards produced? What can increase or decrease this rate? (An acceptable system may take between 1 and 2 minutes to produce a single ID card.)
3. Does the printer create both sides of the cards at once?

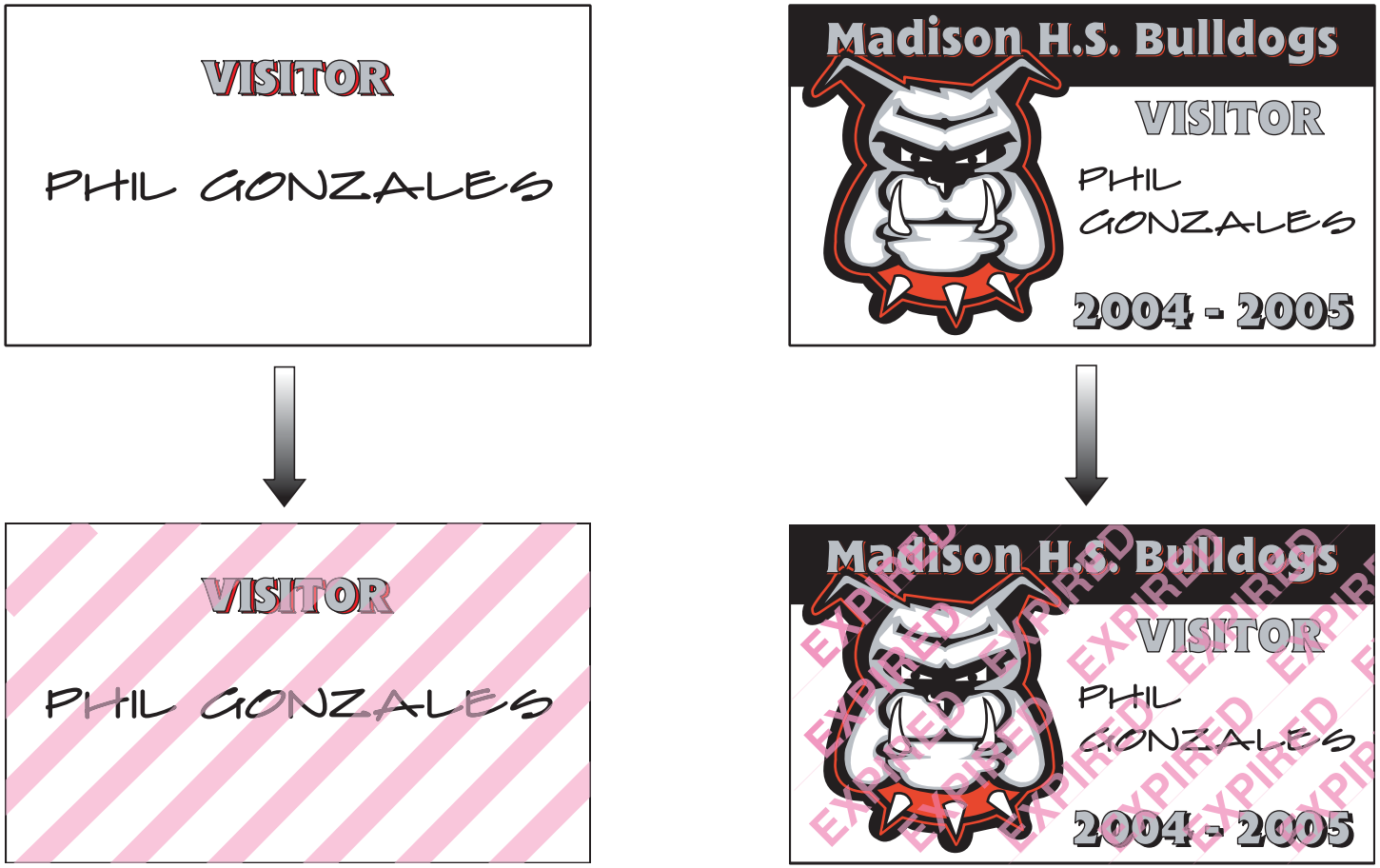


Figure 4.7 The above illustrations show "stock" and custom self-expiring badges upon initial use and after 24 hours.

4. Will the vendor install the system and initially ensure it is functioning properly?
5. Will the vendor program the software for the first card design?
6. 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?
7. What is the maintenance schedule for the printer (i.e., after how many cards?)
8. How long does it take to boot up before it will accept data for the first card?
9. What is the maximum queue length (number of cards) for the printer?
10. 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.)
11. What are the names and phone numbers of schools in your State that are already using this device?
12. How much space is needed for the equipment, operators and waiting students?
13. What happens if the system breaks while registering students?

An excellent way to get more information on the use of badges is to call schools currently using them and ask: How hard is it to use the system, and what difficulties surfaced when implementing it? Is training simple? Have they experienced any equipment breakdowns? What specific improvements have resulted from using ID badges? How many additional blank cards should be purchased for errors or replacements? How often do students or staff forget or refuse to wear their badges and what do you do in response?

References

1. Garcia, M.L. 2001. *The Design and Evaluation of Physical Protection Systems.* Boston: Butterworth-Heinemann; 173, 178-179.
2. Holmes, J.P., Wright, L.J., and Maxwell, R.L. A Performance Evaluation of Biometric Identification Devices. SAND91-0276 1991; 1-29.

Chapter V
Contraband Detection

The ability to detect the presence of dangerous items like weapons and drugs may be necessary in some schools. Schools must decide if detection of contraband items is necessary to accomplish the detection function of the appropriate protection objectives, as described in Chapter 2. An effective contraband detection program can be successful if the correct equipment and procedures are used, and if operators are correctly trained. This chapter discusses contraband detection using metal detectors, x-ray baggage scanners, and drug detection technology.

5.1 How metal detectors work

A metal detector is used primarily to locate specific types of undesirable objects hidden on a person's body. When applied appropriately, metal detectors can accurately detect the presence of most firearms and knives. Unfortunately, they do not distinguish between guns and metal belt buckles. This shortcoming is what makes contraband detection programs problematic and sometimes impractical for many schools, because these determinations must be made by well-trained operators.

A metal detector actually detects any material that will conduct an electrical current. The typical pulsed-field portal metal detectors emit an extremely weak, pulsed magnetic field that produces very small electrical currents in conductive metal objects within the portal archway. These currents, in turn, generate their own magnetic field which is detected by the receiver portion of the metal detector. This type of detection

device is "active" in that it generates a magnetic field that actively looks for suspicious materials or objects.

Counter to intuition, the mass of an object is not important in metal detection. Instead, the magnitude of the metal detector's response depends on the object's size, shape, orientation, electrical conductivity, and its magnetic properties. For example, when a long thin wire is shaped such that no two points on the wire are touching as it is carried through a portal (walk-through) metal detector, it will rarely be detected. However, if this same wire is shaped into a closed circle, the metal detector will most likely alarm even though the mass of the wire has not changed.

5.2 Portal Metal Detectors

This section discusses issues related to efficiently operating portal metal detectors in schools. Issues presented include layout and space requirements, throughput rate, express lanes, hardware and manpower costs, operator and patron procedures, false alarms and sources of interference, performance testing, and working with vendors.

Layout and space requirements

A typical portal metal detector is 7 feet tall, has a floor footprint of 3 feet by 2 feet, weighs less than 150 pounds and is powered by a standard 110-volt wall outlet. The awkward shape of some portals prohibits their being easily moved by one person. Portals are generally freestanding and are only occasionally attached to the floor or surrounding structures. Several layout factors need to be taken into account when installing portals in schools.

First, sufficient space is needed for students and staff (referred to hereafter as "scannees") waiting to walk through the portal. Because students arrive over a very short period of time, a queue line will develop. (You should determine how many scannees will arrive and at what rate, to help determine the expected line or queue length, given the number of intended portals.) There must be enough shelter for the queue of scannees that might build up at any one time such that they will 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 they can be processed; eliminating the opportunity for cutting in line would clearly be important in a school to reduce possible fights.

Unfortunately, the design of most schools does not lend itself to a comfortable staging area for this process. There is usually not enough interior or covered space within the front or main student entrance. This may mandate that the staging area be located further within the facility, which may place some administrative offices or other facilities outside the cleared area. This risk must be weighed when designing the detection program layout.

Second, a significant portion of public schools have multiple buildings and access points to the campus. Few schools can afford to have multiple staffed entry areas with metal detectors. The cost of the

equipment would be high, but not nearly as prohibitive as the manpower to run these multiple systems. Additionally, weapons and contraband can enter a school via non-door access points (windows or open perimeter areas) too. Clearly, the challenge of keeping weapons out of a school extends beyond the front door.

Third, the person waiting in line to use the portal next should be kept back at least 3 feet. This distance avoids sending conflicting signals to the detector. Operators and scannees who have already passed through should remain at least 3 feet from the portal in all directions.

Fourth, space is needed for the scannee to follow procedures. A person about to walk through the portal needs room to place his carried items on the x-ray machine or on a table top for hand inspection and space to pick up these items once through the portal.

Fifth, space is needed for hand-held scan areas and x-ray equipment. Hand-held scanners are needed when the operator can not immediately determine the cause of a portal alarm. X-ray equipment is recommended because contraband items could be hidden easily within purses and backpacks. (See the sections later in this chapter on hand-held metal detectors and x-ray equipment for baggage.)

Sixth, there should be neither space nor opportunity for scannees, including employees, to circumvent the detection system (see Figure 5.1). Very definitive boundaries must be established to prevent circumvention of the system and "passback" of prohibited items from outside the screening area to someone who has already successfully cleared the scanning process.

Finally, 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. These items can easily degrade performance (in the form of multiple nuisance alarms). See the section about sources of interference later in this chapter.

School access during the school day, off-hours or special activities should be tightly controlled to make the contraband detection program effective. Students and others can easily defeat an incomplete or lax system. For example, if the back entrance through the cafeteria remains unlocked and unguarded, then funding and efforts put into a well-meaning program may be wasted. A successful metal detection program generally requires proper funding and major changes to school policies and procedures. These changes may include locking and alarming all exterior doors, bolting window screens, and re-screening students who re-enter after leaving during the day. See Chapter Four on entry control for additional information on limiting access to the school.

Throughput

Throughput is the rate at which scannees are processed. A well-trained operator can generally process 8 to 15 people per minute through a portal

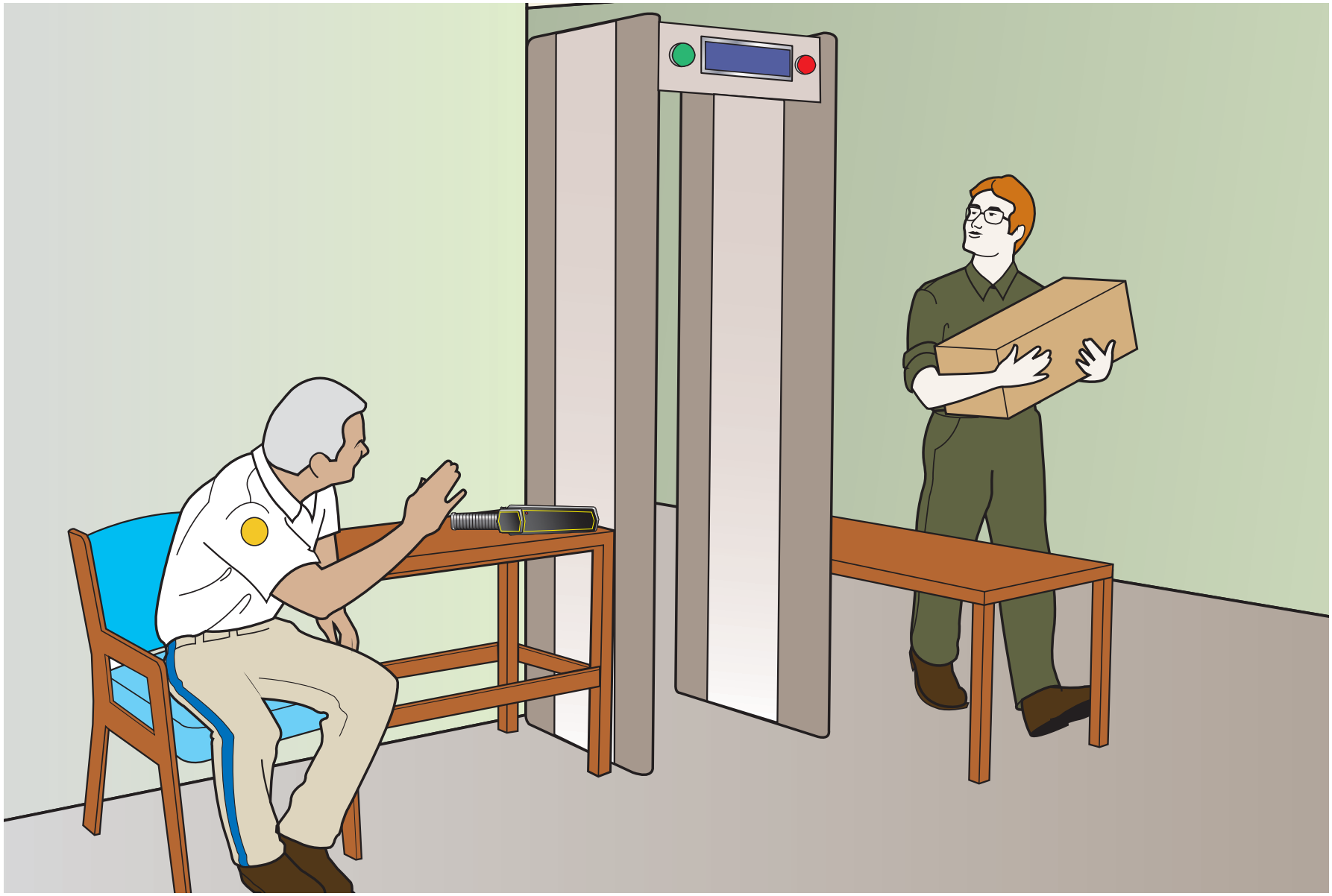


Figure 5.1 Do not allow anyone, including other employees or friends, to circumvent the metal detection system.

detector. This does not include delays for investigating of alarms, or intentional and unintentional delays that could be expected from some students. In the authors' experience, school personnel who have other responsibilities during the majority of the day can process about 10 people per minute.

Assuming operators are well trained, throughput is dependent on:

1. The number of portal devices
2. The rate at which students arrive
3. The motivation of the students to cooperate and move through the system quickly
4. The ability of the school staff to persuade unwilling scannees or have them removed and handled by someone not working within the metal detection system
5. The presence of visitors or who are unfamiliar with the scanning routine
6. How often equipment fails and how quickly backup equipment arrives

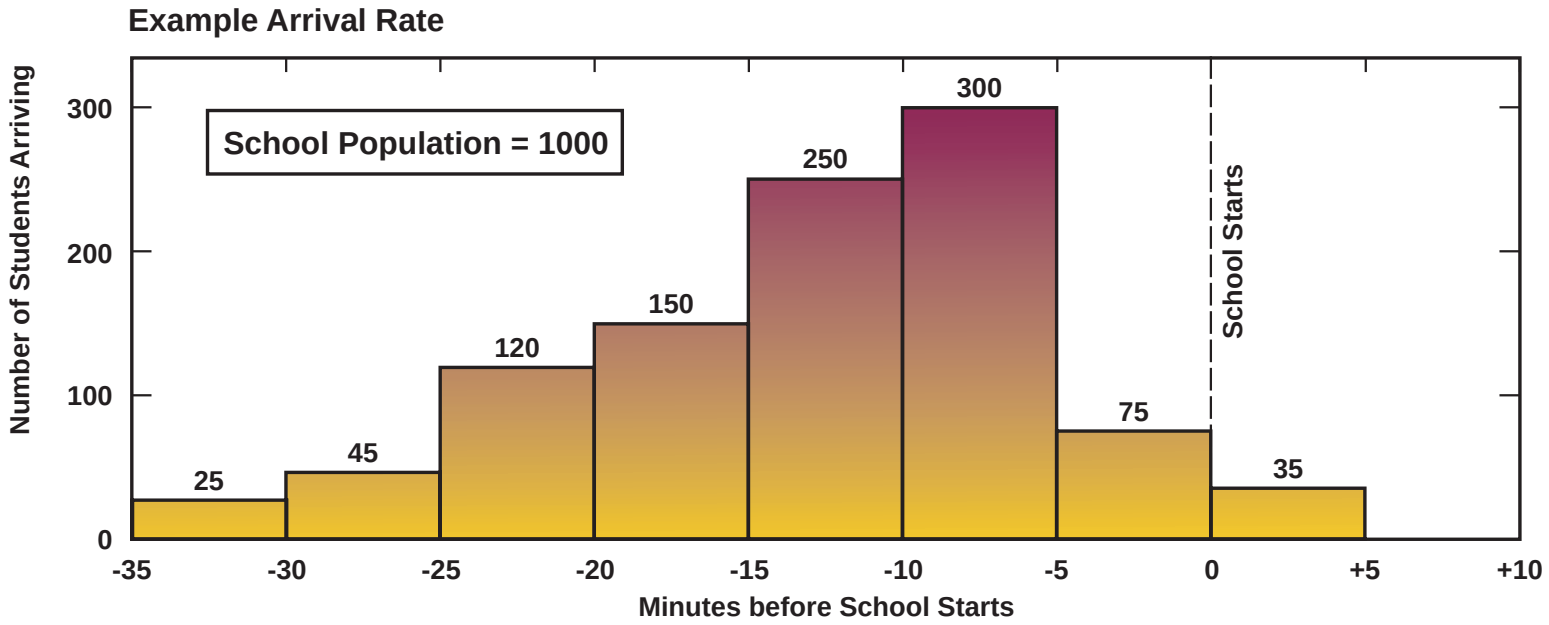
Backup portals can maintain throughput during equipment failures and should not be overlooked. They can be borrowed from the vendor or from a pool of spares shared within a district. In the total scheme of school security, one unexpected morning of allowing all students to bypass the metal detection system may be acceptable, provided that students are not allowed to return to their vehicles nor leave campus at lunch time.

Once the scannee population is aware that they will consistently use the metal detectors each day, they will soon compensate and adjust their behavior. These adjustments will generally be that the population will:

1. Not attempt to take weapons with them into the facility (hopefully!)
2. Learn which acceptable items in their possession will still cause an alarm and begin to leave them at home
3. Adjust their schedule (similar to travelers at airports), perhaps by arriving early enough to miss the main rush

Unreasonably long waits of 15 minutes or more could result in staff, students, and parents alike questioning the need for a metal detector program. Employee organizations may try to bargain for extra pay if consistent, lengthy delays exist.

Figures 5.2 and 5.3 show the average number of students waiting in line (at 5-minute intervals before the start of the school day) to enter the metal detection system for a hypothetical population of 1,000 and 2,000 students, respectively. In this example it is assumed that metal detection equipment is in good working condition, has an optimal layout, that operators are motivated and trained, and students move smoothly through the process. The metal detector is assumed to be the bottleneck of the process and students who fail the initial portal screening are immediately funneled to an alternate screening point and do not reenter or



Expected Queue Build-up

Number of Students Waiting (Scan time - 15 scannees per minute per portal)

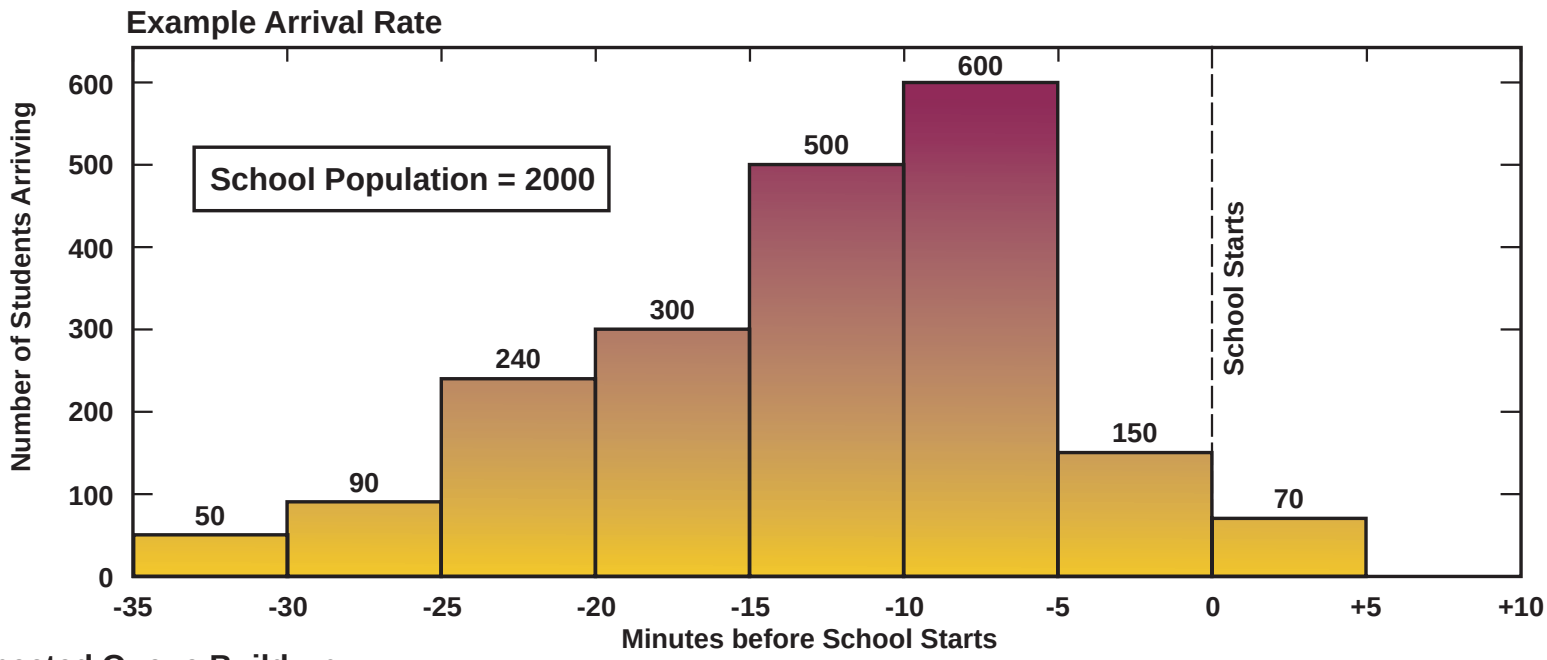
1 Portal	0	0	0	45	120	295	520	520	480	405
2 Portals	0	0	0	0	0	100	250	175	60	0
3 Portals	0	0	0	0	0	25	100	0	0	0

Number of Students Waiting (Scan time - 10 scannees per minute per portal)

1 Portal	0	0	0	70	170	370	620	645	630	530
2 Portals	0	0	0	20	70	220	420	395	330	130
3 Portals	0	0	0	0	6	100	250	175	110	0
	-35	-30	-25	-20	-15	-10	-5	0	+5	+10

Minutes before School Starts

Figure 5.2 ***The graph above illustrates an example arrival rate for a population of 1,000 occupants (students and staff). The table below it depicts the queue length (the number of people waiting) at 5-minute intervals, given 1, 2, or 3 portals with operators who can process people at a rate of 15 or 10 per minute. (Because the arrival rate and operator ability will vary, this chart is for illustration purposes only.)***



Expected Queue Build-up

Number of Students Waiting (Scan time - 15 scannees per minute per portal)										
1 Portal	0	0	15	180	405	830	1355	1430	1425	1350
2 Portals	0	0	0	90	240	590	1040	1040	960	810
3 Portals	0	0	0	15	90	365	740	665	510	285
4 Portals	0	0	0	0	0	200	500	360	120	0
Number of Students Waiting (Scan time - 10 scannees per minute per portal)										
1 Portal	0	0	40	230	480	930	1480	1580	1600	1550
2 Portals	0	0	0	140	340	740	1240	1290	1260	1160
3 Portals	0	0	0	90	240	590	1040	1040	960	810
4 Portals	0	0	0	40	140	440	840	790	660	460
	-35	-30	-25	-20	-15	-10	-5	0	+5	+10

Minutes before School Starts

Figure 5.3 ***The graph above illustrates an example arrival rate for a population of 2,000 occupants (students and staff). The table below it depicts the queue length (the number of people waiting) at 5-minute intervals, given 1, 2, 3 or 4 portals with operators who can process people at a rate of 15 or 10 per minute. (Because the arrival rate and operator ability will vary, this chart is for illustration purposes only.)***

further delay those at the primary entry portal(s). The bulk of students are shown to arrive within a 10-minute window, perhaps resembling a school whose students rely primarily on buses for transportation.

The graphs show the number of students waiting to enter the metal detection process at each time step. The intent of the charts below the graphs is to show the queue length for two different throughput rates. Actual processing time should be between 5 and 10 seconds for most prepared students. Students who are unprepared or set off the alarm and need further screening may require an additional 3-5 minutes of processing time using hand-held detectors and/or manual bags search. This type of analysis could be performed at your school to determine the number of portals needed to prevent excessive queues or tardiness.

After calculating the necessary number of metal detection units, space, and personnel required (and taking unique characteristics of your school into account), the administration may realize the system is infeasible without some changes, given the available resources. Some schools have overcome these limitations by staggering the school day start times for students. This makes better use of limited metal detection resources. Unfortunately, schools that rely heavily on bus service may not be able to utilize this solution.

An alternative: the metal detector portal "Express Lane"

Many inner city schools are driven to perform this ordeal every morning with less-than-motivated security staff and ineffective scanning procedures. In the authors' experience, the result is that hundreds of students are late to class every day. One alternative to the typical metal detection program is a variation that places the responsibility on the students to come to school free of alarm-causing (though usually benign) items or clothing.

This alternative, often called the "Express Lane Method", requires two portal metal detectors at each entrance, at least initially. The first portal or "Slow Lane" uses the normal protocol of placing all book bags and purses through the x-ray machine and hand-scanning any person who sets off an alarm when passing through the detector portal.

The second portal is the "Express Lane". Students desiring to use the express lane are issued a list of items that normally will or will not pass undetected in the portal detector. They are encouraged to use backpacks and purses that will not alarm, or leave them at home, and are shown how items like a large metal ring binder will not pass through, but a smaller or plastic binder will. The same goes for belt buckles, large metal brads on clothing, chains, some types of jewelry, etc. This gives parents the opportunity to make appropriate adjustments to their children's clothing and property before sending them to school. Students who use the express lane move through quickly because their clothing and bags should contain only non-detectable benign items (see Figure 5.4).

Students who set off an alarm in the "Express Lane" are sent to the back of the line of the first portal to

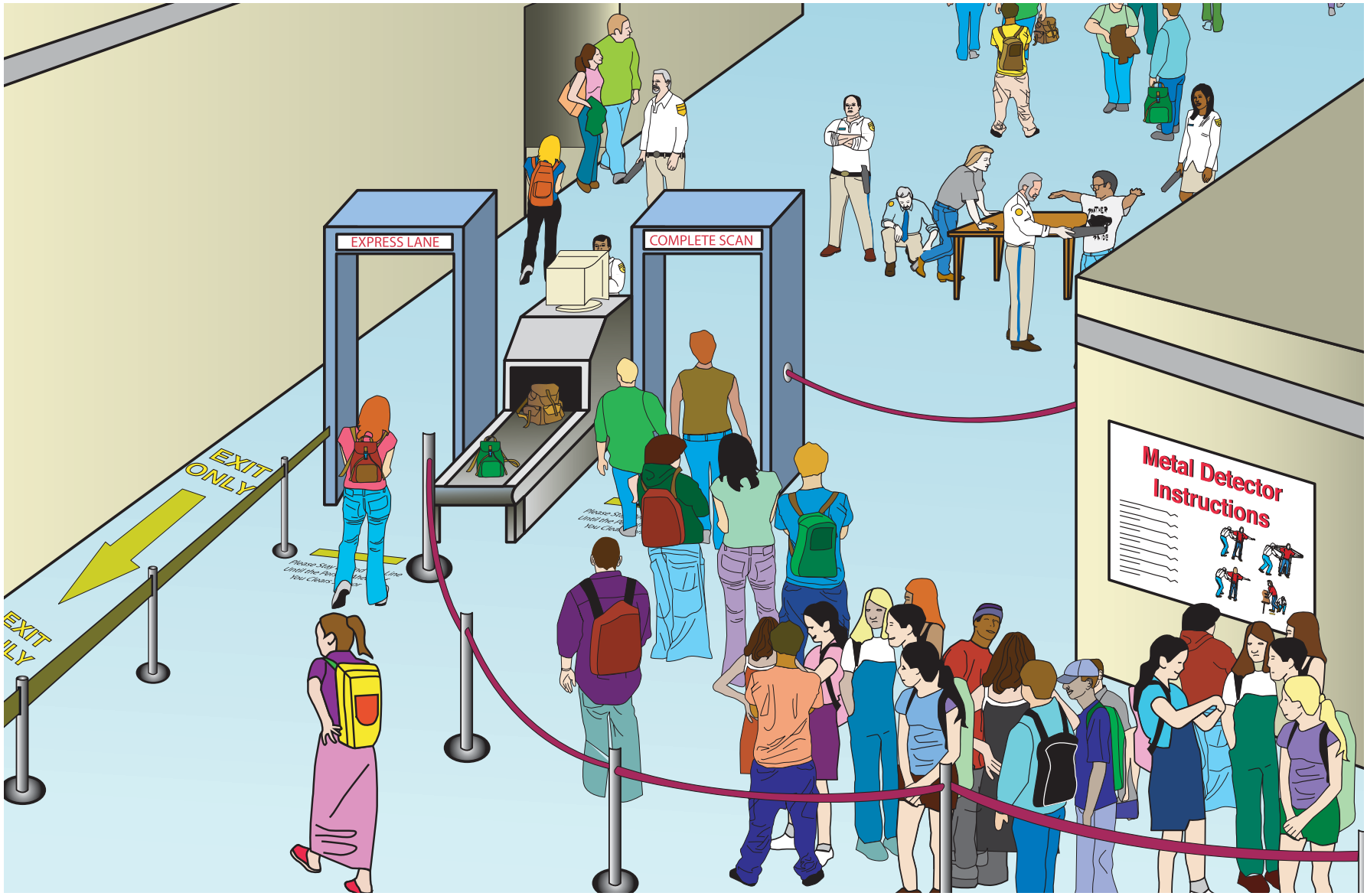


Figure 5.4 ***One alternative for schools to consider for their metal detection program is to set aside one portal specifically for students who have made the effort not to bring in items that would cause the portal to alarm. This portal would be referred to as the "express lane" and would not require students to put their carried items through the x-ray machine.***

be scanned again (purses and backpacks might be dumped and thoroughly checked). The ultimate goal will be that the majority of students and staff will learn and make the necessary adjustments needed to pass quickly through the express portal. Eventually, the "Slow Lane" and x-ray machine may only be needed as backup for visitors, or at special events such as dances and school sports.

Hardware and manpower costs

Moderately-priced portal metal detectors cost around $2,500 to $8,000 and 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. Models above $8,000 generally offer enhanced capabilities that may not be necessary in school environments.

The initial purchase price however is almost insignificant compared to personnel costs required to staff a complete detection program. This fact is illustrated by the successful metal detection program run by the New York City Board of Education in about 50 of its inner-city high schools (see Figure 5.5). For just one of its schools with about 2,000 students and a single entry/exit point, the weapon detection program requires 9 security officers for approximately 2 hours each morning:

1. Two officers operate the two initial portal metal detectors
2. Two officers operate the x-ray machines
3. One officer operates the secondary portal metal detector for students who fail the initial detector
4. Two officers (a male and a female) operate hand-held scanners on students who fail the secondary metal detector
5. Two officers keep students flowing smoothly and quickly and ensure they can not bypass any part of the system.

The only way the NYC schools are able to get everybody to class on time is by a complete restructuring of class periods. First period start times are significantly staggered and students arrive over a 90-minute period. On average, NYC school safety officials estimate that they fund approximately 100 security-officer hours a week for each of their schools using metal detection programs. The next sections discuss efficient procedures for operators and scannees.

Procedures for the operator

Though vendors generally supply basic training and guidelines, it is important to develop specific policies and procedures regarding the logistics of a metal detection program at your school and how to process students who cause an alarm. This section provides some general recommendations on procedures for portal operators; the next section gives recommended instructions for scannees.

The operator should:

1. Conduct a performance test(s) each morning (see the section on acceptance and performance testing) upon turning on the detector to verify that sensitivity settings are correct. This process should take less than 5 minutes each morning

Figure 5.5 ***A photograph of a successful, but manpower-intensive, weapon detection program at a New York City High School.***

for semi-permanent portals. Additional testing (information should be provided by the vendor) will be required for portals that moved into position each morning.

2. Insist that each scannee place his or her feet on drawn footprints at the base of the portal before proceeding. This will ensure that the scannee has not entered the portal so fast that he could have been inadequately scanned.
3. Make certain no other person is located within a 3-foot radius of the equipment while a scan is being performed.
4. Re-scan any person who causes an alarm, even if they can identify what must have caused the alarm, such as a belt buckle or necklace. Confirm that the scannee no longer causes an alarm after the offending item is removed. (Some programs may require a second, more sensitive scan performed by a different portal or with a hand-held metal detector rather than the original portal.)
5. Not be required to adjust control or sensitivity settings.
6. Not allow anyone outside the cleared area to hand something to a person inside the cleared area (Figure 5.6).
7. Not allow familiar, fellow employees or other security personnel to circumvent the system. This is necessary to ensure the integrity of the process. Everyone must be subjected to the program requirements, including students, parents, teachers, maintenance staff, security personnel (except for sworn police officers who are required to carry a weapon), and administrators. To require less would be counterproductive and prejudicial.

Signage is recommended because it provides policy notification and explains the importance of the detectors in maintaining a safe and comfortable learning environment. If needed, 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.

In the authors' experience, students and staff should be given exact instructions and constraints to help the detection program operate efficiently. The instructions should be as short and simple as possible. The following example instruction set could be provided to students and employees in the student handbook and should be posted at the entry to the metal detection area.

Persons waiting to be scanned should:

1. Remove any metal items from their body or pockets and put them in a purse, book bag, or in a provided tray.
2. Place hats, carried jackets, purses, backpacks, and briefcases on the conveyer belt for the x-ray machine (or on the table to be searched by an officer).
3. Stay back from the portal until signaled by the operator to proceed.

Figure 5.6 "Pass-back" of a weapon from someone outside the facility to a person who has already cleared the scanning process is a common defeat method.

4. Walk at a moderate pace through the portal, placing your feet on the footprints at the base of the portal before proceeding.
5. Follow the instructions of the security officer when additional scans are needed.

False alarms

Sensitivity adjustments are generally made by the vendor when the detector is installed in the area where it will ultimately be operational. The optimal setting for your school depends on your unique security goals and what rate of false-positive errors and false-negative errors are consider acceptable.

A false-positive error is an alarm that occurs for an acceptable item, such as a metal key ring. These errors occur more frequently in a program that seeks to err on the side of security. However, false positives can be extremely annoying to scannees, can increase manpower requirements, and result in shorter throughput rates. Constant false-positive alarms may desensitize the operators to alarms, so that they eventually fail to fully investigate the sources of all alarms.

Most portal metal detectors are additive, meaning they generate an alarm based on the total response to all metal detected on a scannee. A scannee with multiple "borderline" items on his body has a better chance of causing a false-positive alarm (see Figure 5.7).

A false-negative error occurs when an unacceptable item, such as a gun or knife, fails to trigger an alarm. These errors may occur more frequently in a program that seeks to err on the side of convenience. This slightly increases the risk of a weapon entering the facility undetected but helps the process run as quickly as possible. In such a program, when an alarm does occur, the operators are more likely to take it seriously and to investigate fully what caused the alarm. Many school metal detection programs operate in this manner.

Sources of interference

Even the best portal metal detectors are susceptible to interference if poorly located. Below is a partial list of possible sources of interference (see also Figure 5.8):

1. Any metal object (such as a stool or trashcan) placed next to the portal
2. Fluorescent lights located directly above the operating area of the portal or within 1-2 feet of the top of the portal
3. Nearby electric motors or other objects that may cause a spike in electromagnetic energy (A large elevator motor can cause interference up to 10-15 feet away)
4. Nearby air ducts in the wall with metal components that expand/contract slightly when the cooling/heating system is in operation
5. Metal plumbing in nearby walls that vibrates when water is running
6. Chain link fencing that vibrates (either from wind or people).

Typical Portal Metal Detector Sensitivities

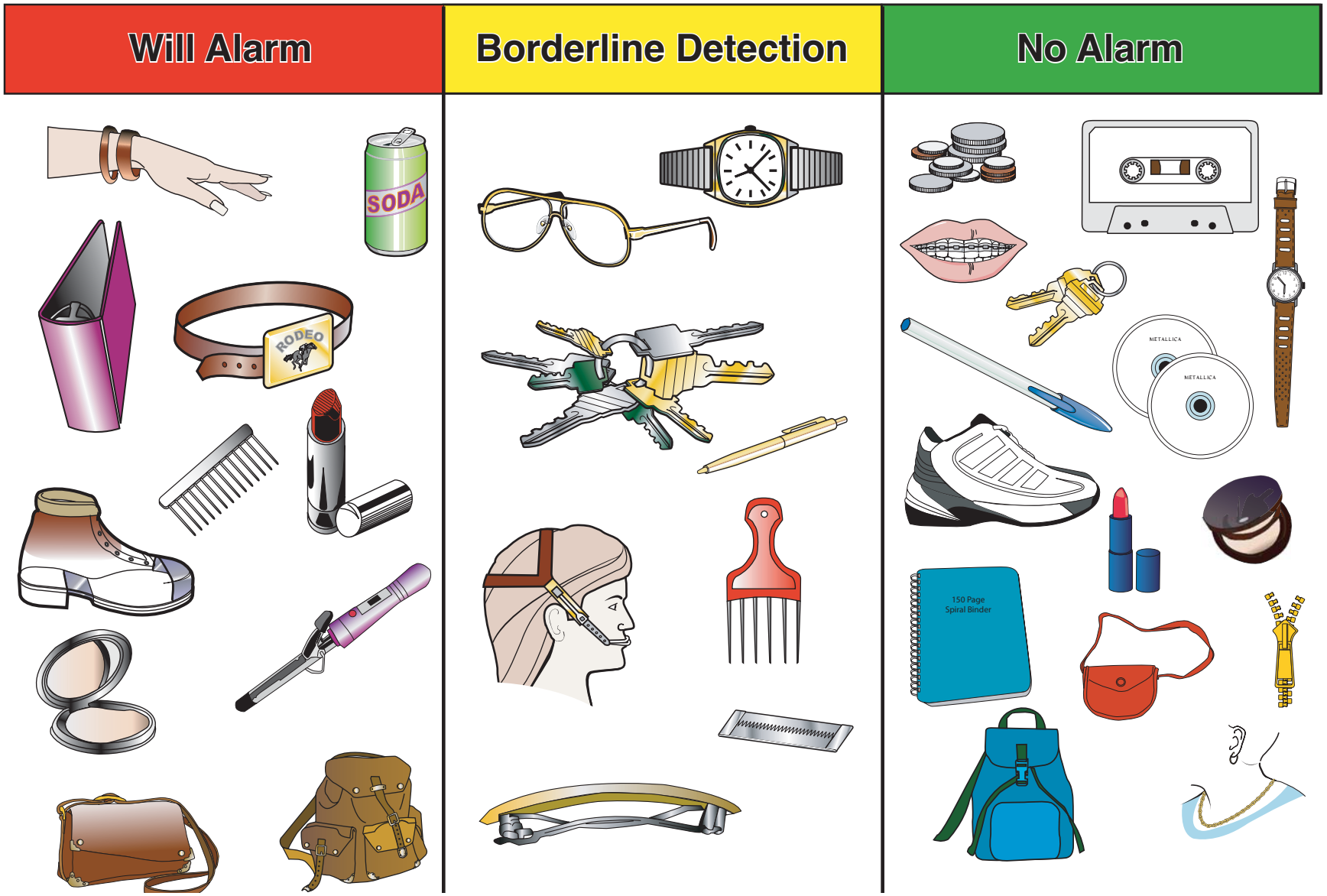


Figure 5.7 This chart illustrates common items and their sensitivity to detection by most portal metal detectors.

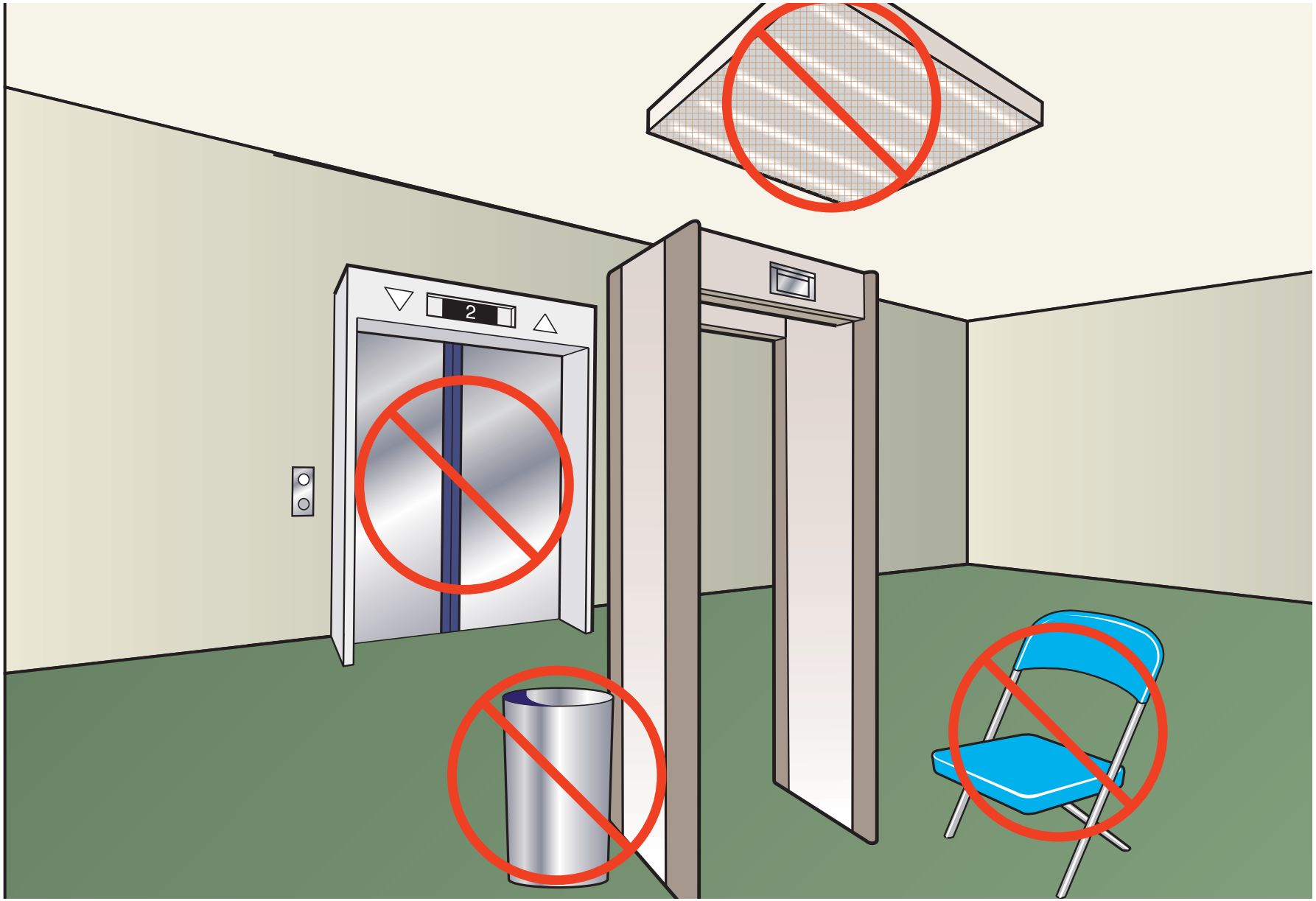


Figure 5.8 ***Portal metal detectors are subject to many sources of electro-magnetic interference that can reduce their effectiveness if not compensated for in the initial programming.***

Most permanent metal structures will not prohibit use of a semi-permanent portal metal detector if sensitivity is set to allow for the anomaly. However, any future change in the portal's position will require a re-adjustment of sensitivity levels.

Acceptance and performance testing

Acceptance testing is a series of tests performed after installation to determine if the device is meeting performance specifications (or your security objectives) as stated in the purchase contract. Every school should run rigorous acceptance tests before accepting or paying for any piece of equipment.

The vendor will also perform tests designed to find the ideal sensitivity settings of the equipment for its location and the contraband items you specify. These tests are repeated after any relocation of the equipment or change to the surrounding environment.

The acceptance tests can be devised with knowledge of the weapons that are likely to be present in any particular community. This varies widely in different parts of the country and can change over time. Your local law enforcement agency can help determine the most likely threats for your area if needed. The performance tests are performed as follows.

1. Determine the three or four most likely weapons for your school. Examples are small handguns, knife with a four-inch blade, brass knuckles, etc.
2. Obtain replica items for each of these weapons from the vendor, the local law enforcement agency, or your school security department.
3. Place these items one at a time on the body of a tester who will walk through the portal with the item placed in various hard-to-detect locations. Good locations to test include: in the hand, up a sleeve, inside a sock on the exterior of the leg, just behind the front of the belt, and on top of the head in a baseball cap. Conduct 10 walk tests per location per item. (In this case it amounts to 10 tests for each of four different weapons, at five different body locations--a total of 200 separate trials! Now multiply this by the number of adjustments needed!) Record the results of each walk through.
4. Determine the three or four most likely borderline items that are acceptable items to bring into the school but that may cause an alarm.
5. Place these items one at a time on the body of a tester who will walk through the portal with the item placed in typical locations (for example, glasses on face, key ring or pocket change in pocket, necklace around the neck). The tester should walk through 10 times with each item and record the test results.

The portal is "accepted" when at least 9 of 10 walk-through tests for each combination of contraband item and position results in an alarm, and at least 9 of 10 walk-through test combinations for each acceptable item does NOT result in an alarm.

In contrast, performance tests are shorter and simpler trials that should be conducted by the

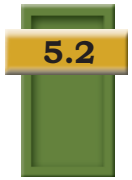
operator of the system at the beginning of each morning before the equipment goes into operation. They consist of walking through the portal four or five times with a piece of metal on different locations of the body. If the portal alarms on each walk-through, then the system is said to be performing well and is ready for operation. If the system fails these tests, and no obvious reason for these failures is evident, the device should then be taken out of operation until serviced.

Selecting a vendor

Vendors may be willing to come to your school with a detector and perform a demonstration if you are considering purchasing one. Have the vendor set up the portal in the area you expect it will ultimately be placed, and adjust the sensitivity to what he considers the optimal settings. After this point, the demonstrator should not be allowed to adjust these settings further.

You should then run your own set of tests using volunteer students with weapon replicas normal borderline items on their body. After two or three such demonstration sessions by different vendors, most law enforcement agencies or school security departments will develop a familiarity with portal metal detector features and what their own application may require.

When issuing a bid for a portal metal detector, a school should require in the RFQ that a bidder meet a series of performance tests, such as those defined in the section on acceptance and performance testing. The author recommends specifying that the vendor will not be paid until the requirements are met. Language in the contract should allow the school to withdraw the contract if the chosen vendor fails to meet these obligations within 2 or 3 weeks after initial installation.



Hand-held metal detectors

Battery-operated, hand-held metal work quite well (Figure 5.9) and are an important compliment to portal detectors. Commonly used in airport security, they can accurately locate conductive materials on or in a person's body. As with portal detectors, they do not discriminate between contraband and benign materials and are only as good as the operator using it. It is the responsibility of the operator to investigate and determine the cause of any alarms.

While it is easy to learn to use a hand-held metal detector correctly, school administrators should not underestimate the value of annual training for operators and staff who 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.

Though hand-held metal detectors are very affordable (normally less than $200), it is not feasible to screen scannees using only hand-held detectors, because throughput is only two students per minute. The hand-held metal detector is best used as a supplement to portal metal detectors to

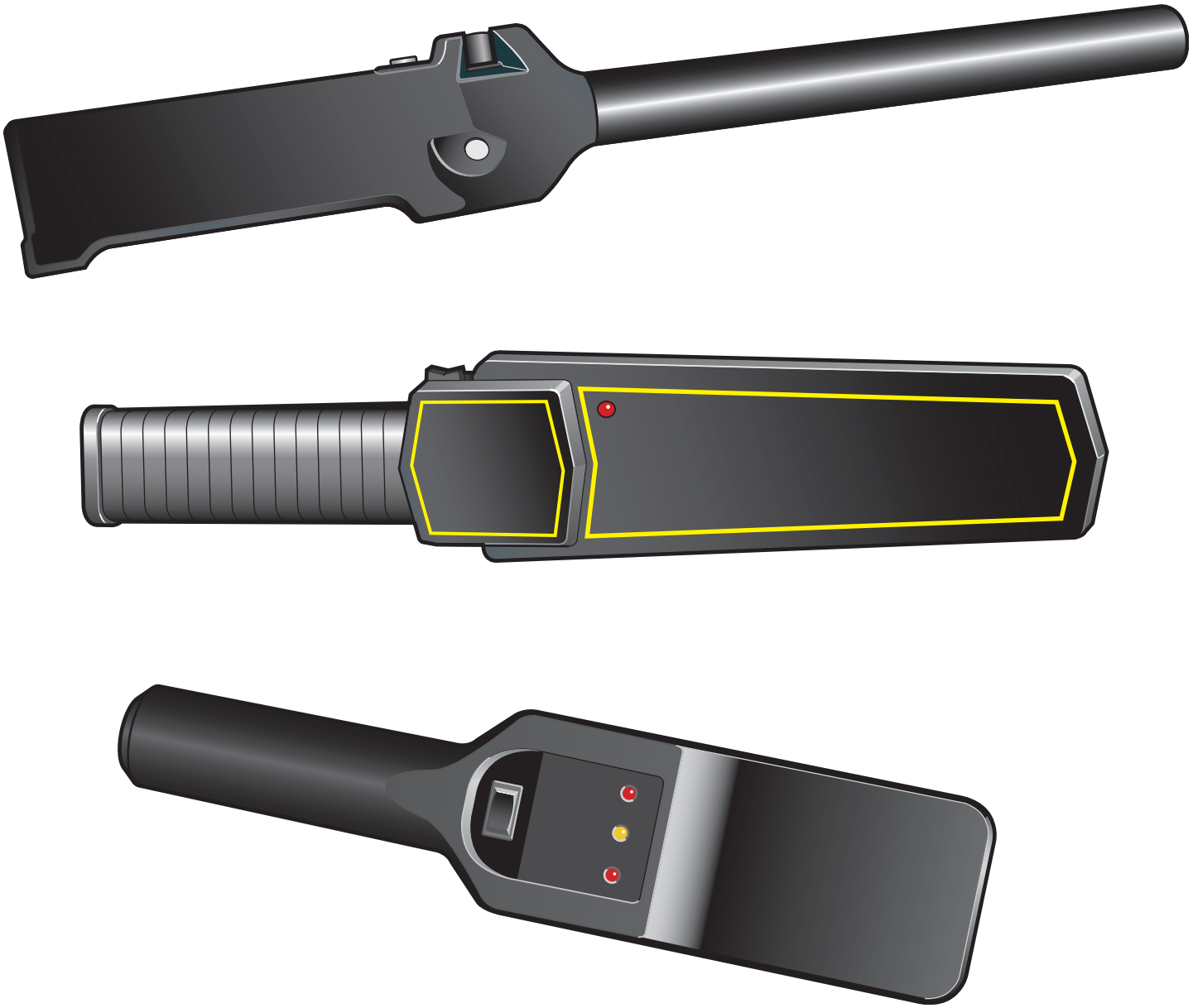


Figure 5.9 This illustration depicts a variety of hand-held metal detectors on the market.

accurately locate the source of an alarm, after a student has already walked through a portal system and caused an alarm.

Some schools intend to use hand-held metal detectors only for random spot checks on student. In the authors' experience, this is an ineffective method for locating weapons for 2 reasons. First, it is very difficult to get a truly random scan. Second, even if the scans are intended for only a small, distinct group of higher-risk students, they will object (rightfully) to being singled out over lower-risk students. Further, they can easily defeat the search by forcing other student to carry contraband onto campus for them. One successful approach is to choose an entire classroom at a time and scan every person (including the teacher) in the room.

Another approach that may keep weapons off campus is to establish a policy stating that a metal detection scan is required of any student who arrives more than x minutes late. This may provide excellent deterrence if students, if only to convince them to not be late, to prevent having their personal items searched by an adult.

One school in downtown Boston reported to the author that they enforce a policy in which any student found roaming the halls during class, or even seen roaming the halls on the video surveillance system, is subject to a complete search using a hand-held detector. This search includes emptying all pockets. Not surprising, the students in this school now avoid hall roaming.

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 sensitive only to within a few inches of the device's detection "paddle." A 6- by 6-foot area should be sufficient for the actual scanning process. It is also necessary to have a table or other stable structure for purses and book bags for students to lean on when they lift their shoes to be scanned. (See the sections containing procedures for the operator and scannee.)

Scanning should not 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 metal detection procedures should be performed in plain view of others. One unusual exception is when a person is suspected of hiding contraband in a more private area of the body.

Throughput

Accurately scanning individuals that are unfamiliar with the process may take as much as one or two minutes, especially if there are multiple alarm sources per person. However, after the program has become routine, it should take no more than about 20 seconds to scan an individual with a hand-held detector. Assuming there are no difficult or ambivalent scannees, most schools can plan to hand scan two people per minute per operator.

It is good practice to explain procedures to parents, staff and students often, so they become routine.

Instructional posters located at the scanning equipment should include diagrams of how a scannee should stand. In the authors' experience, students need about 2 weeks to acclimate themselves a full-scale metal detection program in which they are scanned daily. During this time they learn to arrive a few minutes earlier and wear clothing and accessories that are less apt to cause an alarm.

Hardware and manpower costs

Hand-held metal detectors range in price from $20 to $350. Schools should plan to spend between $125 and $200 for detectors that have desirable features, including

1. A long detection paddle (to reduce the number of passes across a person's body)
2. A warning light or beep when the batteries are beginning to run low
3. An audible feedback alarm that is loud or high in pitch for larger items and soft or lower in pitch for less suspicious items (such as a zipper).

Hand-held metal detectors run on either a 9-volt battery or rechargeable NiCad battery. Each will last for approximately 1 hour of constant scanning. (It is suggested that batteries be removed when not in use or when detectors are infrequently used.) One 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 hand-held metal detectors. As mentioned in the section on throughput, a trained operator can scan approximately two people per minute. It is recommended to have both a male and a female operator of hand-held detectors for scans on students of both genders.

Procedures for the operator

Proper operating policies and procedures for hand-held scanning should be tailored if needed to special needs or characteristics of your student and community population. The following are some recommended policies and procedures for the operator:

1. Pass the detector over the scannee's body at a distance of no more than 3 to 4 inches. Avoid touching the body or clothing with the detector.
2. Set the detector at its highest sensitivity setting unless there is significant interference from nearby materials that will cause constant alarms.
3. Perform the scan in the same pattern each time so it is known what parts of the body still need scanning. A sample routine, illustrated in Figure 5.10, follows:
   a. Ask the person to empty their pockets and place all carried items on a table (manual baggage search procedures are not covered in this text). The person should stand about 2 feet in front of the table on footprints drawn on the floor, with his feet about 18 inches

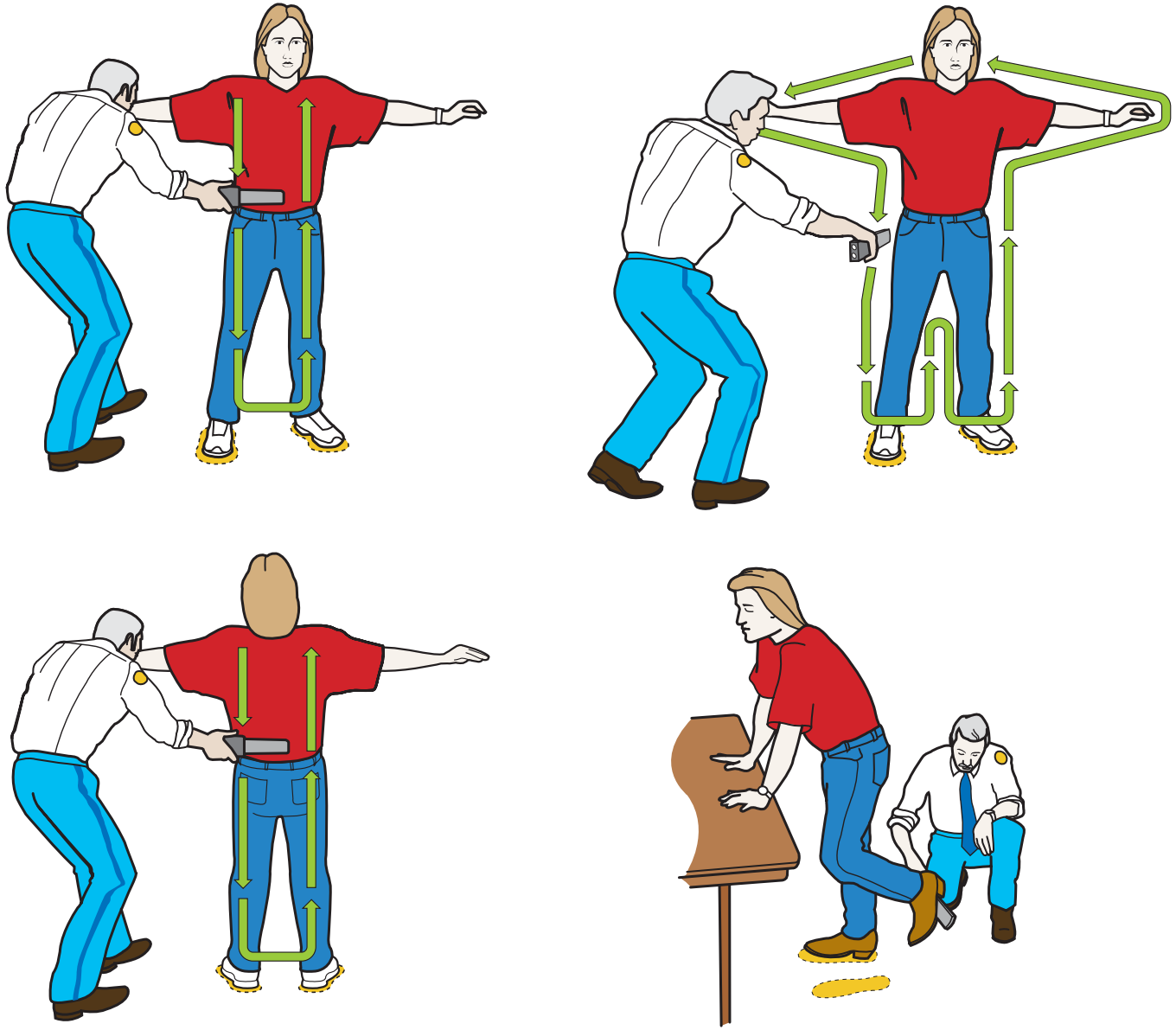


Figure 5.10 This is an example of procedures for using a hand-held metal detector that has at least a ten inch zone of detection.

apart, facing away from the table. Ask the scannee to hold his arms out to the side, parallel to the floor.

b. Quickly test that the scanner is working properly by running it across something conductive on the operator's body, such as a belt buckle.

c. Start at the top front of one shoulder of the person. With the paddle of the detector held horizontally and parallel to the front of the body, sweep down and back up the body as shown in position A of figure 5.10. (If the detection paddle is less than half the width of the body being scanned, the pattern will have to be modified to achieve adequate coverage.)

d. Keeping the paddle horizontal but parallel with the floor, sweep the detector paddle as shown in position B of Figure 5.10. It is particularly important to avoid touching the person's body with the paddle when scanning between the legs.

e. Ask the person to drop their arms and turn around. Scan the back of the body as shown in position C of Figure 5.10.

f. Ask the person to grab the edge of the table for support, then to lift one foot up in back of him or her. Scan across the bottom of the shoe as shown in position D of Figure 5.10. Shoes and boots with steel shanks or toes should cause a short squeal from the detector. If an equivalent squeal is not heard from each shoe, the scannee should be instructed to remove the shoes for a manual inspection.

g. For the head area, start at the top of the forehead and scan around the top of the head down to the back of the neck. (This procedure is usually implemented only in schools where large hair styles are common or where razor blades are a popular weapon.)

4. The operator should be able to distinguish between the detector responses to small innocuous items such as zippers, and large suspicious items (many detectors respond with a variable pitch and/or volume based on object size and shape).

5. When there is no visible source for an alarm (clothing is shielding the source object), ask the person to show you what they have in that area. For example, for an alarm along the arm or wrist, have the person pull up his shirt sleeve. Re-scan directly over the visible item.

6. Do not let the scannee influence you as to what is causing the alarm (see Figure 5.11). For instance, if the detector denotes the presence of a suspicious item under a shirt sleeve, completely investigate the source of the alarm even though the scannee assures you that it is just a watch under the sleeve that is causing the alarm. Similarly, the operator should not stop the scanning process after finding the source of one alarm – there may be multiple alarm (contraband) sources.

7. The lower abdominal area is difficult to scan because this area is private in nature and metal items are usually found there: belt buckles,

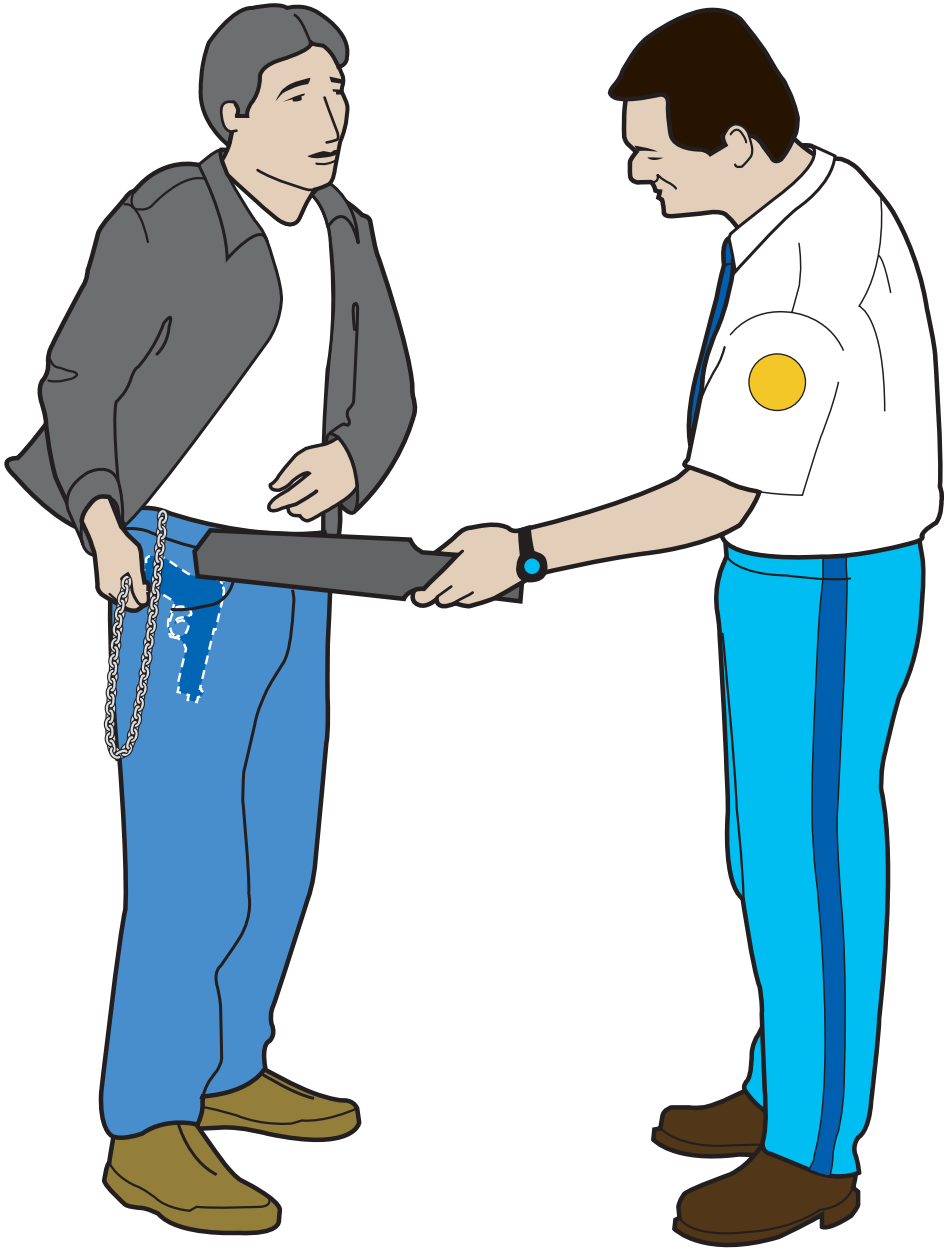


Figure 5.11 Here, the scannee is attempting to influence the operator by claiming that the chain is causing the alarm, when, in actuality, there is a hidden weapon.

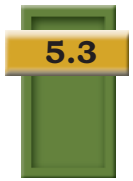
buttons or snaps, and zippers. If an alarm occurs in this area, there are two possible ways to further investigate:

a. Ask the scannee to undo their belt and pull the ends away from the middle of the body. Now re-scan the zipper area. The feedback volume from your hand-held metal detector should tell you if it is now only sensing a zipper and/or a metal snap, or if a more suspicious item is present and further investigation is still needed.
b. Ask the scannee to twist the front of their waistband forward, to ascertain if anything is hidden behind it. This may require private facilities where further investigation can be accomplished in the presence of two or more school employees of the same gender as the scannee.

Selecting a vendor

If issuing an RFQ for hand-held metal detectors, it is recommended that the contract require the detectors to have the following features:

1. A variable pitch of alarms that provides more information to the operator. For example, a softer squeal for an innocuous item, like a zipper, and a louder squeal for a bigger, more suspicious item.
2. A detector paddle or zone that is at least 10 inches long.
3. A signal that indicates the battery is beginning to run low, as opposed to an abrupt termination of operation.
4. Rechargeable batteries.



X-ray baggage scanners

Metal detectors are usually not effective on purses, backpacks, briefcases, or suitcases because they normally contain many metallic items or construction materials, resulting in many nuisance alarms. If your security objectives call for scanning of these items, consider using an x-ray scanner.

Sensors in X-ray scanners collect the magnitude of the radiation signal passing through baggage, and display the resulting image. Materials with higher “Z” numbers block more of the signal. (A "Z number" is the atomic number of an element. A low Z number in x-ray scanning terms is any material with an atomic number less than 26, such as aluminum. A high Z material has an atomic number greater than or equal to 26, such as iron, copper or silver.) Most black-and-white monitors can display images in positive or negative (light or dark) objects. There are two types of color systems on the market. A colorized single-energy (one radiation source) system arbitrarily assigns color based on the level of energy transmitted through the material. The second type is

a dual-energy (two radiation sources) system that assigns color based on the effective Z-number of the material. The first type is less expensive but adds little useful information to the display. The second type adds useful information but is normally cost-prohibitive for most schools (Figure 5.12).

Safety concerns

For the single-energy unit types that are appropriate for school applications, a vacuum tube emits x-rays downward through baggage as it is automatically moved through the equipment. Sensors detect the magnitude of the received signals and the resulting images are transferred to a TV monitor. An operator must carefully examine each image for evidence of firearms, knives, or other contraband.

Today's x-ray machines for baggage use a pencil-thin beam of low-energy radiation that is well-shielded. The beam generally scans back-and-forth across a piece of baggage as the baggage moves beneath it. Infrared (IR) beams installed within the equipment can accurately start and stop the x-ray beam source so that the x-rays are operational only when a piece of baggage is located in the imaging position.

Modern x-ray scanners are very safe and the health risk to the operator and general public is negligible. In fact, radiation exposure to operators from baggage scanners has been shown to be only a few microrems per hour, which is equivalent to standing in the sunlight for only a few minutes. The U.S. Food and Drug Administration has approved much higher doses of radiation for normal food preservation methods. Most scientists feel that the FDA is quite conservative in the limits it has established. Additionally, photographic film is not damaged in modern x-ray scanners because the dose is so low.

Setup and space requirements

A typical x-ray baggage scanner will have a footprint of about 4 by 4 feet in size. This does not include any type of conveyor belt to automatically move items into and out of the x-ray imaging area. The smallest recommended conveyor belt for a school application is 8 feet in length, which would add about 2 feet on either side of the scanner itself. Conveyors can come in almost any size; typical conveyors for airports are a total of 10 to 12 feet in length.

Unlike portal metal detectors used for personnel, x-ray baggage scanners are not sensitive to their surroundings. You should have the vendor install, set up, and calibrate the x-ray scanner. After installation, moving the equipment to a different location is generally not a problem. While the equipment should not be abused, it is not overly delicate.

Throughput

The expected throughput of an x-ray baggage scanner will depend on two things: the efficiency of the operator and the amount of clutter in a typical bag. Carried purses and backpacks that contain many detectable items (metal rulers, tools, metal tins and foil-wrapped items) can significantly slow

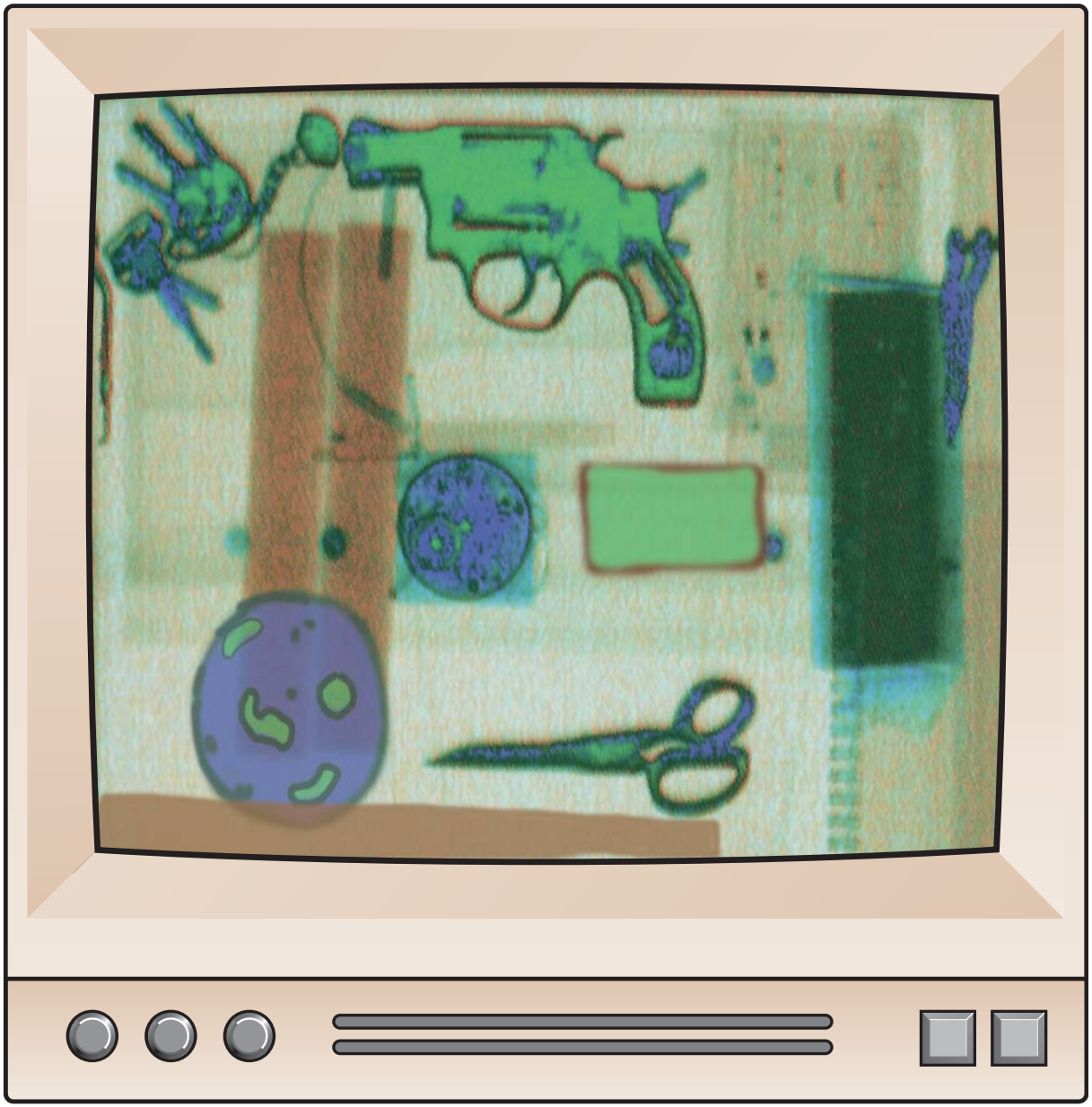


Figure 5.12 This is an example of the monitor from a dual-energy x-ray machine that assigns color based on the effective z-number of the material. This is an informative system but normally too expensive for schools.

down an operator examining each piece of baggage. Speed can increase if the operator becomes familiar with individual students and the objects they usually carry.

Generally, between 10 and 20 items per minute can be examined using an x-ray baggage scanner. As many as 30 items per minute can be effectively scanned if most of the items are benign (that is, they contain no obvious metal items larger than a coin or button) and are not touching in the image. Dense clutter within a bag will necessitate that bag be pulled off the conveyor and be manually searched.

Vendors will normally provide initial training at no expense. Some training aides include prepared images of baggage passing through a scanner, which can be played back on a VCR and TV monitor for operator practice. Another feature on some equipment will randomly superimpose the image of a suspicious but fictitious item over actual images during the normal work time. These phantom images help prevent operators from being lulled into complacency by the routine absence (hopefully) of prohibited items.

Hardware and manpower costs

Single-energy (one radiation source) x-ray scanners which are appropriate for school environments cost about $30,000. Some models add the convenience of a color monitor, although this may not provide any additional information to the operator for decision making. There are much more expensive models on the market, but these are generally used in conjunction with explosives detection. The detection of drugs is possible, but in the authors' experience the sophisticated equipment needed is too expensive for most schools. The conveyor belt needed to feed items into and out of the x-ray scanner will generally be priced as part of the total system cost.

The manpower cost for operating x-ray equipment is very high. It is generally recommended that one operator work exclusively at the monitor of an x-ray machine no more than 2 hours at a time and preferably no longer than one-half hour at a time. Schools, like airports, should have at least two operators per x-ray scanner. This allows operators to alternate responsibilities (watching the monitor and performing manual baggage searches) every half hour.

The difficulty in schools is that, like metal detectors, a sufficient number of x-ray scanners and operators are needed during a relatively short period of time to maintain acceptable throughput during the morning rush. While easy to hire one security aide to work 8 hours a day, it is difficult to find eight security aides to work 1 hour a day. It is not unusual therefore, for schools to use properly trained administrators, teachers, and other employees to supplement the security personnel operating the equipment each morning.

In the authors' experience, at least eight security personnel are normally required to support a complete contraband-detection program at a school with 1500 to 2,000 students, provided that class start times are staggered). This assumes the school

is using

1. Two x-ray machines (staffed by one person each)
2. Two portal metal detectors (staffed by one person each)
3. An additional portal for those who fail to pass one of the first portals (staffed by 1 person),
4. Two hand-held metal detectors for those who fail the second portal (staffed by one male and one female who can also perform hand searches if necessary
5. One person to oversee and keep the whole process moving.

Additionally, someone is needed to operate the equipment the other 7 hours of the school day. This might be an expensive effort with minimal returns. Some schools enforce a policy in which entrance doors are basically locked one-half hour after school begins in the morning. Although this is a rather harsh stance, it may be necessary in a school where resources are limited and the threat of weapons is quite high.

Recommended Procedures

Operation of an x-ray baggage scanner is straightforward and vendors will provide recommended procedures. Each school can tailor procedures to their own environment if needed. The challenging part of operating x-ray equipment is knowing what to look for. An untrained and unmotivated operator can negate any possible benefit that might be gained in a weapon detection program. Some recommended procedures for operators of x-ray scanners are:

1. Orient baggage on the conveyor as instructed by the vendor, because different models transmit and receive radiation signals at different angles (orientations).
2. Watch for solid dark objects (if display is set this way) that could be a weapon, part of a weapon, or hiding a weapon, as baggage passes on the screen. This is particularly difficult when a weapon is oriented such that the viewing angle (top, bottom, or end) disguises its familiar features and shape. This is why proper training is essential.
3. Manually search baggage if clutter prevents resolution of individual items. Clutter occurs where several items of similar z-numbers are grouped together in an x-ray image, such that the actual size and shape of each item cannot be reasonably determined without a manual search.
4. When in doubt about an object in a bag, investigate.

Surprisingly, band instruments can be put through an x-ray machine (provided they fit inside the machine). The thickness of most metal instruments will allow the x-ray scanner to see within and behind the instrument. The author recommends testing x - ray equipment before purchasing with various band

instruments to determine if any of them (or their cases) will be a problem for the machine.

Hopefully students will learn to leave items at home that trigger an alert to the operator of the x-ray equipment. This may not be the case for disruptive students, who may go out of their way to slow down the system. School administrators can prepare consequences in advance, in the event this behavior continues.

Educating students and parents in advance regarding which items that will result in bag searches can help speed up the process at the beginning of a scanning program. However, do not share information regarding the system's weaknesses and what makes it difficult to recognize weapons. This information should remain restricted to appropriate school and law enforcement personnel responsible for security.

A simple set of instructions located at the x-ray scanner can remind students quickly of what is expected of them. For example, the sign (which assumes a school that is also using portal metal detectors) might read:

1. Place all detector-sensitive items (large jewelry, watches, belts with metal buckles, large key rings and loose change) in your backpack or purse.
2. Lay all books, notebooks, purses, bags, lunches, backpacks, coats and electronic devices on their widest side on the conveyor belt. *(Adjust according to whatever orientation is best for your school's equipment.)*
3. Do not stack items; place them on the conveyor belt separately.
4. You can easily reduce the chance of security personnel manually searching your belongings by eliminating clutter.

The author recommends another sign on the other side of the x-ray scanner stating:

Please immediately check for all of your personal valuables and possessions. The school is not responsible for any lost items. If you have valuable or irreplaceable items, please do not bring them to school.

Acceptance and performance testing

The author recommends that schools use a test procedure defined by the American Society for Testing and Materials (ASTM, 2005) for their initial acceptance testing, and that they incorporate it into their regular performance testing. The test uses a 10-step wedge of milled aluminum (Figure 5.13). Across the bottom of the step wedge are several wavy wires of different gauges. The x-ray scanner is performing well if 10 different shades of gray are clearly distinguishable and a certain number of the wires are also seen, when the step wedge is scanned in the machine. (A very good x-ray scanner will see even the smallest gauge of wire behind the thickest step of the step wedge.) A step wedge will be

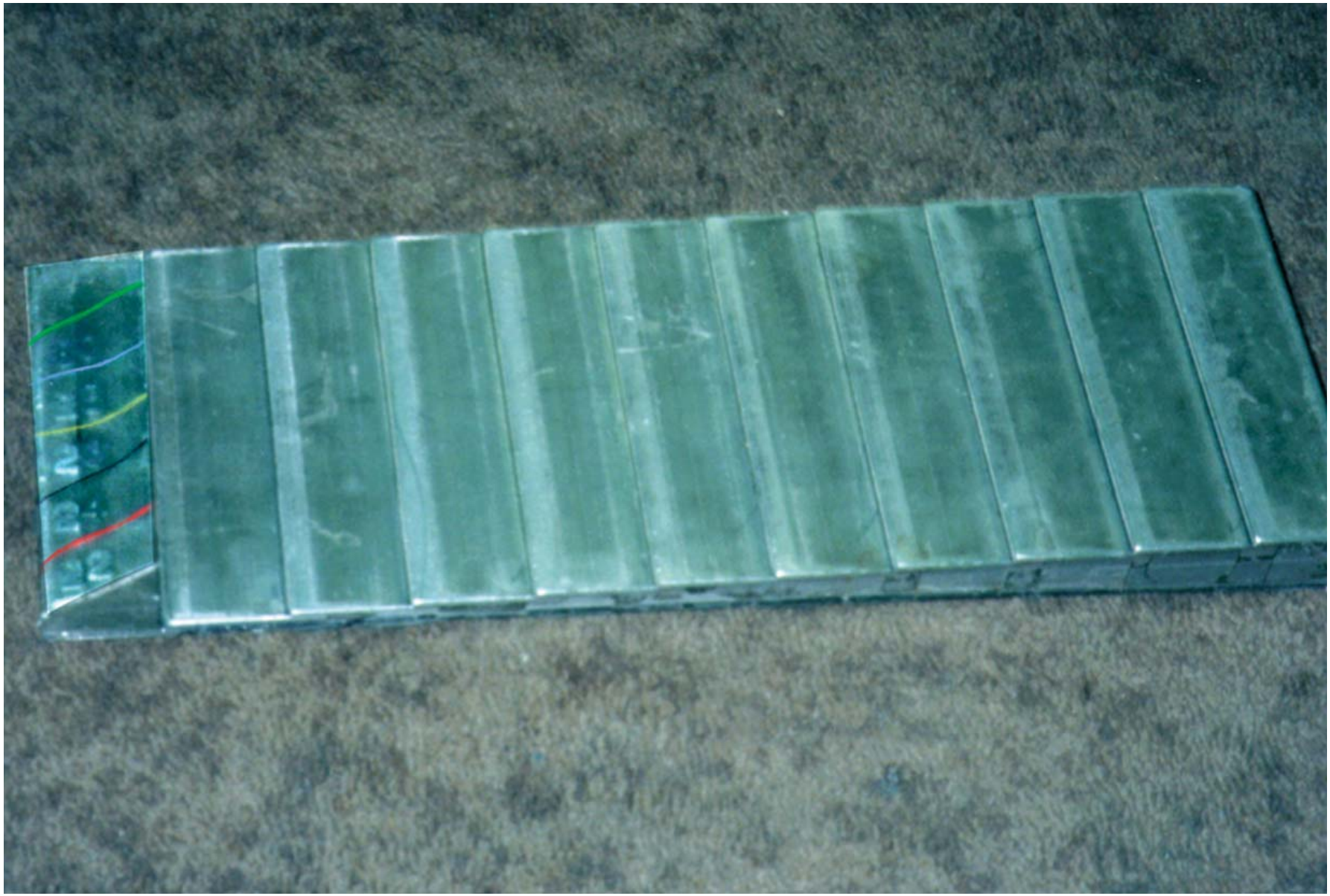


Figure 5.13 This 10-step wedge is used for x-ray baggage scanner acceptance testing and regular performance testing.

available through your vendor, who will likely employ the same tool for its own testing purposes.

The test should be performed initially to accept the equipment and regularly thereafter (once a month), to verify that the system is performing well. A decrease in the number of visible wires over time may indicate that the unit needs repair or adjustment.

Maintenance and expected lifespan

Maintenance requirements are very minimal for modern x-ray equipment. The largest moving part, the conveyor belt, is often self-oiling, and the oil reservoir may only need occasional filling. Vendors may recommend periodic procedures to test for radiation leakage, though the chance of such leakage is very low.

Most companies offer extended warranties or maintenance contracts for x-ray baggage scanners. Service contracts are generally more expensive than expected repairs over the life of the equipment without a contract. However, some schools may want to establish a service contract up front, when funding is available and earmarked for such expenses. In the absence of such a contract, schools should contact the factory when repair is needed.

Most x-ray baggage scanners will have a life of 10 years or more. During this time, it is reasonable to expect to replace the vacuum tube that is the source of the x-rays. In the authors' experience, x-ray scanners are more susceptible to obsolescence by technology advancements than by equipment failures.

Selecting a vendor

There are several excellent products on the market appropriate for use by schools. A school security person or administrator should take the time to visit one of the national trade shows where this equipment is on display. Seeing the equipment and talking with vendors can result in a better understanding of products you are considering, and can help identify potential vendors.

In the authors' experience service is the most distinguishing feature between vendors, because most x-ray scanners appropriate for schools are priced similarly, operate easily and have good quality images. If a service contract is being purchased, it may be possible to include language in the RFQ requiring the vendor to provide service and repair within 3-5 work days or to substitute a backup system within 48 hours. This would be difficult however in rural locations. If your school district intends to purchase several units for multiple schools, the district may be able to negotiate an excellent price that will include a backup unit stored by the district.

Drug Detection

Many administrators report that they consider illegal drugs a problem at their schools. It is arguable whether or not the presence of illicit drugs constitutes a security issue in the same sense that vandalism, assault, or theft do, and administrators must make this determination. It certainly undermines safety. If drug detection is an objective of the security system,

a determination must be made as to which protection objective is most appropriate (see Sections 2.2 and 2.3), and which method of detection is most feasible. It seems unlikely that a security system can prevent illicit drugs from ever entering the campus, but it may be possible to detect and apprehend those who bring them. This is turn will provide a deterrent effect that should prevent some drugs from arriving on campus. This section will briefly discuss trace versus bulk detection, considerations in choosing a detection technology, and recommended detection methods for schools.

The National Institute of Justice (NIJ) has published an extensive and useful guide in 2000 titled, "Guide for the Selection of Drug Detectors for Law Enforcement Applications" that explains in detail the different types of drug detection methods available, their performance against various drugs, and current commercial sources for detection equipment. While some progress has been made in the development of drug detection technology since its printing, it still covers the major types of detection technologies that are commercially available. Therefore, schools who are considering procuring drug detection capability are encouraged to read the NIJ guide for further information on the specific types of technologies available.

Trace vs. Bulk detection

Drug detection systems typically fall into one of two categories: (1) trace detectors, and (2) bulk detectors. In bulk detectors, the item to be screened is normally irradiated with some sort of incident radiation to detect large quantities (such as a pound) of contraband substances in baggage, packages, or hidden on the body. The radiation that is transmitted, backscattered, or emitted from the contraband material is subsequently collected and analyzed, often resulting in an image (NIJ Guide 601-00). Trace detectors perform a chemical analysis of a vapor (air) or particulate sample and can identify the chemical compound, such as heroin or cocaine. Trace detectors can determine if items or people have been contaminated by drugs, though it is not possible to determine whether the contamination occurred through direct or indirect contact. Many trace detection systems are based on ion mobility spectrometry (IMS) technology, which has been used to make rugged, portable equipment available for use in the field. Trained canines are also trace detectors and can in principal be trained to detect any type of drug. Technology-based trace detectors operate in either a vapor or swipe sample collection mode (Shannon and Hammond, 2003).

Portable air samplers or "sniffers" are available for detecting drug vapors emanating from larger quantities (several ounces) of drugs. Sampling the air adjacent to a solid mass of a drug allows drug vapor to be collected. However, some drugs, such as Heroin, produce very little vapor, making it difficult to detect trace amounts.

Surface particle detectors can be employed in the "swipe" mode if drug vapors are not present (due to the absence of larger quantities of drugs). Using a cloth-like collection medium, the operator swipes the

surface of the item of interest. The sample is then inserted into the detector so that the collected particles can be extracted, analyzed, and identified (Shannon and Hammond, 2003).

Considerations in choosing a detection system

Many factors should be considered when selecting a drug detection system including (but not necessarily limited to) the following: purchase cost; maintenance costs; throughput rate (related to screening speed); sensitivity of the system to different types of drugs; system portability; items (people, bags, lockers or vehicles) to be screened; ease of use, including training and maintenance requirements; associated safety and environmental issues. Additionally, if the system is to be used to screen people, human factors that might interfere with the use of the system and legal concerns, such as invasion of privacy or search and seizure issues, should be considered (NIJ Guide 601-00).

Above all, it is important to consider the specific applications for which the system will be used. For instance, will it be used primarily for checkpoint screening or for more wide-ranging searches, and will it be used primarily for screening people, hand-carried articles, mail, vehicles, lockers or backpacks? Prior to making a purchase, it is highly recommended that buyers consult with product vendors and, if possible, past customers of the vendors who have purchased the system in question. Existing users are an excellent source for unbiased information on product performance and usefulness.

There is no such thing as a "one size fits all" drug detector, and compromises among the characteristics listed above will be necessary. Therefore, schools must decide which screening applications and performance characteristics are most important to their security program.

Recommended detection methods for school environments

Most drug detection technologies will probably be too expensive for schools, though large districts may have sufficient funding. (Bulk detection systems can cost up to one million dollars or more.) The most useful commercial benchtop systems for schools are likely to be trace detectors based on ion mobility spectrometry (IMS). IMS is one of the most widely used techniques for trace detection of illicit drugs and other contraband materials.

A number of features of IMS make it attractive. The technique has probably been more widely developed than any other trace technology for drug detection. Compared with other technology-based drug detectors, IMS systems are moderately priced, with several systems in the $30K to $50K range. Maintenance costs vary from system to system, but are not large in most cases. Most of these systems are portable enough that they could be moved in the trunk of a vehicle and only a few hours of training are needed to operate them. These instruments have response times of only a few seconds, the proven ability to detect a number of key drugs, and audio and visual alarms that tell the operator when a drug has been detected and the type of drug. The most

effective means of collecting a sample for presentation to an IMS is surface swiping, but vacuum collection of samples is also possible for most systems (NIJ Guide 601-00).

One problem with trace detection in general is that trace amounts of drugs might be present even if a student or staff member has not actually handled or used drugs. Furthermore, particulate contamination is easily transferred from one surface to another. A person who has handled cocaine will transfer cocaine particles to anything else they touch, including skin (perhaps by shaking hands with someone), clothing, door handles, furniture, and personal belongings.

Completely removing particulate contamination from an object requires rigorous cleaning, and, in the case of bare hands, a single thorough washing may not be sufficient to remove all particles. Particulate contamination is so tenacious and easily spread, that a large fraction of the $20 bills in the United States are contaminated with enough cocaine residue to yield positive detections with some trace detectors (NIJ Guide 601-00).

Knowing this, if trace amounts of drugs are detected on a student, what should a school do about it? A positive detection only indicates the person has either recently been in contact with a specific drug, or that surface to surface particulate contamination has occurred. The detection probably does not constitute sufficient evidence for prosecution or discipline, though it would certainly raise questions. Further, it would not indicate the source of the trace material (i.e., the location of the bulk material), or whether the person has brought bulk quantities onto campus. Additional investigation would be required to yield conclusive evidence, and schools must determine if this is feasible.

One alternative to the technology based systems is to use a trained drug sniffing canine. Dogs have proven to be very effective at locating some of the most widely abused illicit drugs, including (but not limited to) marijuana, methamphetamines, cocaine, heroin, hashish, and opium. A canine could very rapidly screen a whole row of lockers at a school, and if properly trained, would likely alarm only on macroscopic amounts of narcotics instead of traces. Further, canines can follow a scent gradient directly to its source, a capability which does not exist in any current technology-based system.

Canines have their drawbacks as well. A handler is required, and a dog can typically work for only a few hours before requiring a break (although this is probably just fine in school environments). This is in contrast to many technology-based systems that, in principle, can operate 24 hours a day. Additional minor disadvantages of canines are that the dog cannot tell the handler what type of drug it has detected, and the dog's performance may vary somewhat due to health and weather conditions. Finally, dogs are not usually used to screen people because some people fear dogs, and a liability exists if the dog bites someone.

The costs of a dog and a handler are substantial, but very large school districts might be able to afford one. Procurement costs for a single dog are typically near $10K depending upon the supplier and the dog's level of training. (Care needs to be taken to only obtain dogs from reputable sources.) The main costs associated with purchasing and maintaining a canine are the training costs, especially the salary and other overhead costs associated with the handler. These can be quite large. The Federal Aviation Administration has estimated that the cost of maintaining one properly trained officer/canine team at a major U.S. airport is approximately $165K per year. Most of this cost is the salaries and overhead associated with the handlers. Although this figure is probably higher than that of a typical officer/canine team maintained by a local law enforcement agency or school, it demonstrates how maintenance costs associated with a canine can add up (NIJ Guide 601-00).

A good option for most districts might be not to purchase a dog, but to establish an agreement with local law enforcement to periodically use one of their drug sniffing dogs. It might be reasonable to ask the local police force to bring in a trained dog once or twice a month at unannounced times to do checks of lockers. The police might be willing to do this for free or a minimal cost, since it would be good public relations and might even be viewed as part of their normal work.

References

1. ASTM F792-01e2, "Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems," ASTM International.
2. Parmeter, J.E., Murray, D.W., and Hannum, D.W., Guide for the Selection of Drug Detectors for Law Enforcement Applications, National Institute of Justice, NIJ Guide 601–00, August 2000.
3. Shannon, G.W., and Hannum, D.W., "Illegal drug detection in mail to inmates at the Pima County jail", SAND2003-1954C, p2.

Chapter VI
Intrusion Detection

Intrusion detection is simply the process of "noticing" that someone is attempting to enter an area, usually after hours, which they are not authorized to enter. An effective intrusion detection system is a vital component in a comprehensive security program that notifies after-hours security personnel that a break-in is in progress. This report only covers interior sensors, because exterior sensors are more expensive to operate, tend to require specially prepared environments to work effectively, and are normally only used at high-security facilities. This chapter discusses the intrusion detection process, performance characteristics of sensors, types of interior intrusion sensors, and recommendations for sizing and installing the detection system.

An intrusion detection system is an integral part of most school security programs. It provides notice of potential theft of computer equipment, band instruments, or maintenance equipment and tools. It helps safeguard student records (an important privacy issue), teaching materials, and even the safety of the night custodial crew as they are working.

Perhaps the most important benefit of an adequate intrusion detection system is the increased ability to interrupt vandalism. If someone were to break into a school, say, over a long weekend, they could cause irreparable damage if left to their vandalizing without interruption. Many break-ins have left classroom interiors literally destroyed, and some vandals have concluded their visit by setting the school on fire. It can be incredibly difficult to recover from this type of incident which negatively impacts the school-year calendar, district finances, and morale.

6.1 The intrusion detection process

An effective detection system supports a process that ultimately ends in a proper response to the alarm. The process steps are:

1. Detection
2. Alarm Communication and Display
3. Assessment
4. Delay
5. Response

Detection is the capability to notice (or detect) an intruder trying to gain unauthorized access into an area or building. In most office buildings, government facilities, and schools today, small sensors are installed in strategic locations of the building interior. The sensors look for certain conditions such as motion or a change in the thermal energy of an object or area within a room.

After an intrusion is detected, it must be **communicated**, or transmitted, to someone who is prepared to react in some way. This communication first travels via wire, cabling, or through RF (radio frequency) to a panel that receives the alarms at the site. The panel then uses phone lines, cell phone, pager, or direct cabling to further transmit the alarm condition to locations such as:

1. A school administrator's home phone (or beeper number)
2. The police station
3. A nearby security person who may even live on the campus, or
4. An alarm-monitoring company.

For electronic intrusion detection systems, the communicated alarm must then be **displayed** to the person or organization that receives it. This display will also be an electronic component — a computer monitor, a pre-recorded phone message, or an alphanumeric pager message. An exception to the electronic communication and display component could be a system that simply initiated an audible, local alarm. The intent in this case is to alert someone in the immediate vicinity to take action. The Table 6.1 compares silent versus audible alarms.

Once the alarm has been displayed to the appropriate person, the alarm must be assessed to determine what caused the alarm condition. The best type of assessment is when a facility has a video surveillance system that is configured to display images remotely of the area in which the alarm occurred, usually via a special web site. If a person can view a few seconds of pre- and post-alarm images of the area in which the detection occurred, they can quickly assess the alarm. The source of the alarm might be a poster falling off the wall, a cat locked in the building, a balloon popping, or an unauthorized person entering the facility.

Another type of electronic assessment consists of microphones installed throughout the target facility. When the monitoring company receives an alarm,

Silent alarms	
Pros:	Cons:
Neighbors are not bothered by the noise.	Neighbors will not hear the alarm and are less likely to witness intruder activity.
The intruder will not know that he has been detected. This increases the chances that a responder will apprehend the intruder.	If it takes a long time for the police to respond (which is not uncommon due to the large number of false alarms that occur), the intruder has a lot of time to steal or vandalize school property.
The intruder cannot determine at what point the sensor was tripped or how to avoid detection in the future.	
Audible alarms	
Pros:	Cons:
Alarm may scare off the suspect before he accomplishes any theft or vandalism.	The intruder will usually not be caught.
Knowing there is an active alarm system may serve as deterrence to other potential intruders.	Neighbors may be annoyed if there are many false alarms, especially in the middle of the night.
Neighbors may notice suspicious activity and hopefully will report it.	The intruder can "probe" the system by intentionally setting off the alarm repeatedly to learn its capabilities.
	The intruder may "probe" until the school or police turn off the "problematic" system, then make a major raid on the facility without quick response.

Table 6.1 A comparison of silent and audible alarms.

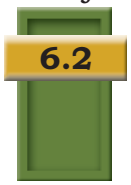
they can "listen in" via the microphones. In this way, they may be able to determine if a person is actually in the facility. If the recipient of the alarm information does not have access to video or audio from the facility, then they are generally forced to have the police or a security contractor travel to the site to determine if a break-in has occurred.

Introduction of **delay** mechanisms or measures increase the chances of actually intercepting an intruder before he/she can escape. Any measure that will slow down the intruder, requiring more time to accomplish his/her mission will decrease the probability of the intruder's success. Examples of delay methods are:

1. Locking doors and windows
2. Bolting valuable equipment to the floor or to a table, as appropriate
3. Using multiple layers of protection, such as placing student records within a locked cabinet within the school's locked walk-in vault within a locked room within a locked building inside a closed perimeter of campus fencing
4. Using padlocks that are resistant to bolt cutters

After assessing the alarm and confirming that it is an actual intruder, some action must be taken to stop the incident in progress. This **response** would consist of confronting the suspect(s), perhaps pursuing the suspect(s), and then making an arrest (or calling the police and holding the suspect until the police arrive).

It is considered very dangerous for a non-police officer or other untrained person to attempt to respond to an alarm. Even police officers are often instructed to not enter a school or other facility to assess an alarm by themselves. Some responders have been murdered by an intruder who was originally just intent on theft. Furthermore, if a school district is aware that the principal, coach, or a neighbor is designated as the responder, the district could incur a large liability if the responder is injured or killed.



Performance characteristics of sensors

Intrusion sensor performance is described by three fundamental performance characteristics:

1. The probability of detection, (P_D)
2. The nuisance alarm rate, (NAR)
3. Vulnerability to defeat

The P_D for an intrusion sensor is always less than one (1.0), since there are no perfect sensors. Manufacturers usually perform repeated tests on their sensors to be able to report the P_D at a given confidence level (C_L). For example, if a manufacturer states values for P_D and C_L of 90% and 95%, it means that they are 95% confident that the sensor detects intrusion at least 90% of the time, based on tests they performed (Garcia, 2001). However, the probability of detection can vary with the

1. Target (i.e. whether the intruder is walking, running, crawling, etc)
2. Sensor design
3. Sensitivity setting
4. Weather or environmental conditions
5. Condition of the sensor (maintenance)

The NAR is the frequency of nuisance alarms over a given amount of time. A nuisance alarm is any alarm not caused by an intrusion. Sources of nuisance alarms include electromagnetic, acoustic, thermal, meteorological, seismic, and optical effects and small animals (including birds and insects). A false alarm is a nuisance alarm caused by the sensor, such as from poor maintenance or a component failure (Garcia, 2001). Some common sources of nuisance alarms in schools are mobiles hanging from the ceilings, floating balloons, and loose papers disturbed by the HVAC system at night.

Nothing is more annoying for a police department than to dispatch two officers to a school which has transmitted an alarm, only to discover that the alarm was caused by some benign source such as a bird trapped in the building, a heat register that blew some classroom decorations around, or for apparently no reason at all. Police stations are beginning to either charge for their time in responding to a nuisance alarm or even refusing to respond to alarms altogether.

Most types of sensors have a sensitivity adjustment which affects the NAR. If set to the highest sensitivity, a sensor will tend to produce many nuisance alarms because it will detect the slightest disturbance. If set to the lowest sensitivity, a sensor might fail to alarm during a real intrusion. The author strongly recommends that the vendor test the sensors once installed, to determine a setting which minimizes the NAR but yields an acceptable level of detection. Additionally, as the number of sensors in the system increases, so does the overall possibility for nuisance alarms. Each school should have someone assigned to keep the sensor system well-maintained after the initial installation and sensitivity adjustments.

6.3 Types of interior intrusion sensors

There are several types of intrusion detection sensors that are effective for school applications. Each type operates well in the appropriate environment, but no single type of sensor is appropriate for all locations. Your vendor should determine which sensor best minimizes nuisance alarms while assuring detection of true alarm conditions in each location. These sensors are presented below with a discussion on sources of nuisance alarms, strengths and weaknesses, and important installation considerations. If additional information is needed, excellent reviews of interior sensors have been written by Barnard (1988), Cumming (1992), and Rodriguez (1991). Adams (1996) has published helpful information related to sensor selection and operation issues.

PIR Sensors

PIR (passive infra-red) sensors are the most commonly used volumetric (i.e., protecting a volume of space, rather than projecting a single beam) motion sensor. (Active infra-red (IR) sensors, which project a single "line" or beam, are not discussed in this manual. An example of an active IR sensor is the transmitter and receiver pair installed across the bottom of a garage door opening for safety purposes. Multiple active IR sensors in a column can create an IR "fence" that is invisible to the naked eye, as dramatized on TV in spy shows.)

PIR sensors use pyroelectric detectors that receive thermal heat energy in a room or area. The pyroelectric detector converts changes in thermal energy it receives, which results in an output of an electrical signal proportional to the change in thermal energy. The pyroelectric detector is most sensitive in the range of thermal energy emitted by humans. This thermal range, however, includes most "warm things", such as animals, heaters, sunshine, etc.

The detection zones of an average PIR look somewhat like multiple "fingers" extending out from the unit (see Figure 6.1). Walking parallel to the PIR detector across a number of these finger zones causes the PIR to see changes in thermal energy and then alarm. A PIR sensor is less sensitive to objects moving directly toward the sensor. Some types of PIR sensors allow the user to set the number of fingers which must be crossed before the sensor will alarm. Sources of nuisance alarms for PIR sensors may include small rodents, birds, floating mylar balloons, insects within the sensor casing, and heat registers and radiators.

The following are vulnerabilities of PIR sensors:

1. If the sensor view is completely blocked (intentionally or not) by furniture, tape on the sensor, etc., it will not detect motion at all.
2. Hair spray or paint applied to the lens of the PIR may partially or fully block its view so that the sensor will not function properly.
3. If a room is kept at a higher-than-normal temperature, sensitivity can be reduced.
4. It is possible for a perpetrator to by-pass a PIR by moving very slowly across the field-of-view. Note: This is so slow that most people don't have the patience or the ability to remain that still for that long.

The following are important installation guidelines for PIR sensors:

1. Do not install PIR sensors close to or next to a vent, as temperature differences between the ambient and vented air may cause nuisance alarms.
2. Do not aim the detection volume to include a possible heat source.
3. Do not aim a PIR at a window because sunlight or passing clouds may result in a temperature change that the sensor would detect.

Figure 6.1 This diagram illustrates the detection zones of a PIR (passive infra-red) sensor.

4. Make certain that the detector unit is completely sealed to keep insects out.
5. The best installation locations are where an intruder is forced to cross multiple fingers (parallel to the detector) upon entry.
6. For valuable intruder targets (such as computer labs or where student records are stored), consider installing two PIRs to "self-protect" each other with overlapping coverage.
7. Read the PIR specifications before purchasing. Normally PIRs will come with information regarding the field-of-view and the maximum detection distance. These distances will change with temperature fluctuations.
8. Some PIR manufacturers include stickers, or decals, to apply to the PIR lens to "mask out" certain areas within the field of view where it is not desirable to have detection. Examples of these types of areas are where a heater vent is, where the classroom guinea pig cage is, etc.
9. PIR sensors cannot see through glass, furniture, objects, or walls.
10. Some PIR sensors attempt to alarm only on certain sizes of detected items. These units make the decision to alarm using proprietary software that discounts a rodent but alarms on a human body.

Microwave sensors

Microwave sensors are a type of volumetric motion sensor that transmits a low-power microwave field that is reflected off objects in the room. Detection is based on the Doppler frequency shift that occurs between the transmitted and received signals caused by motion in the detection volume. Microwave sensors are most sensitive to motion directly toward the sensor, not across its field-of-view.

The following are important installation guidelines for microwave sensors:

1. Eye damage can occur if the microwave if viewed directly at a range of ≤1 foot when the unit is turned on.
2. Microwave fields can transmit through glass, dry wall, and other light construction materials. This means that authorized movement in a hallway immediately outside a locked, sensored room will register as an alarm.
3. Heavy concrete or cinder block walls will prevent transmittal of microwave fields through them. A room with heavier construction material with metal doors and no windows is an appropriate application for microwave sensors.
4. A few microwave sensors have a range adjustment to allow their use in a room with light construction.

Sources of nuisance alarms for microwaves may include:

1. Movement of metallic objects, such as a Mylar balloon or a mobile made of tin foil;

2. Fluorescent lights, though some microwaves have a filter that cancels out the frequency of flickering fluorescent lights;
3. Birds, somewhat susceptible to crawling rodents, slightly susceptible to insects;
4. Movement outside a sensored room, especially if the walls are of light construction or glass.

Dual-technology sensors

Sensor units that consist of both a microwave and a PIR sensor are referred to as dual-technology (dual-tech). Dual-tech sensors are usually configured such that both detectors must to detect motion within a certain time window, usually less than one second, in order to alarm. This arrangement can significantly reduce nuisance alarms. The probability of detection for dual-tech will be somewhat lower than for the individual sensors, but it is generally felt that this is more than compensated for by the reduction of nuisance alarms.

Magnetic switches

Magnetic switches are inexpensive sensors for doors and windows. They consist of a reed switch and a magnet, one of which is mounted on the door frame and one on the door. The reed switch changes state when a magnet is close to it, pulling the contact within the reed switch closed, thereby completing the circuit. When a door (or window) is opened, the magnetism is removed and the contact pops open, thereby breaking the circuit and creating an alarm.

Magnetic switches can be simply defeated by introducing another magnet, if the installation allows access to the switch. Additionally, worn out or poorly maintained doors can cause magnetic switches to give nuisance alarms (see Figure 6.2).

A balanced magnetic switch (BMS) is a more sophisticated type of magnetic switch that is more secure and harder to defeat. It uses a bias magnet installed in the switch unit that, in conjunction with the door magnet, forms a balanced magnetic field around the reed switch when the door is closed. When the door is opened, the removal of the door magnet causes the bias magnet to pull the reed switch into the alarm state. Introducing an additional magnet would upset the balanced magnetic field, thereby causing the reed switch to go into alarm.

BMS sensors are very dependable, with few sources of nuisance alarms. Disadvantages of the BMS are that the devices are somewhat bulky, unattractive, and more expensive than a traditional magnetic switch. However, they are very effective intrusion detectors for doors.

The following are important installation considerations for balanced magnetic switches:

1. It is important to read all of the manufacturer's specs regarding alignment and spacing of the unit.
2. Before installation, make certain that the door latch, strike, and hinges are in good working order and properly aligned. After installation of the BMS, changes to other parts of the door mechanism could result with nuisance alarms or a constant alarm state.

Figure 6.2 The dirt that was allowed to build up in this high school auto body shop caused the garage door magnetic switch to nuisance alarm on a regular basis. The alignment of the switch could also have been a problem.

3. For installation on a metal door or frame, non-ferrous material is needed to act as a spacer between the door and the BMS.

Glass break sensors

Glass break sensors serve as a type of boundary protection – the initial detection of an intruder before he enters a facility. For a school setting, they can also provide an alarm to authorities that multiple windows are being broken, a common vandal prank. There are two types of glass break sensors:

1. Acoustic/audio – These sensors are mounted on a wall and listen for the sound of breaking glass. These sensors can be located up to 25 feet from the glass source. However, window coverings can alter the acoustics of breaking glass, which hinders PD. Acoustic glass break sensors are susceptible to several sources of nuisance alarms; one is the odd noise an extended metal tape measure makes.
2. Vibration – This type of sensor must be attached directly to the glass of each individual window of concern. The sensor responds to vibrations typical of breaking glass. Vibration sensors are more reliable than acoustic sensors, but are unattractive, and an intruder can easily see them.

Wireless sensors

Wireless versions of the PIR, microwave or dual-tech sensors discussed above are convenient where ceiling access is difficult or long cable and conduit runs are too expensive. These sensors are generally powered by batteries that must be replaced every two to five years. As discussed in Chapter 3.3, inclement weather, transmissions through walls, fences, vehicles or trees, and exceeding the maximum recommended transmission distance may degrade signal performance.

A good wireless system should include a supervisory feature that regularly checks the status of the entire system. This includes checks for low batteries of sensors, as well as reporting of any tampering, such as where a sensor cover has been removed.

The main advantage of using a wireless system is its easy installation. The disadvantage includes the need to replace sensor batteries, and the possible loss of alarm signals due to interference by other RF signals or to purposeful shielding.

6.3 Sizing and installing an intrusion detection system

The size of a school intrusion detection system is driven by the need to protect assets as determined by the process outlined in Chapter 2. The larger the system that is required, the higher the cost will be. The cost is driven by the number of sensors, the installation, and the number of zones employed. Sensors are usually the cheapest part of the system, and installation costs are usually the most expensive.

Each sensor (except for the more technically challenging RF systems) will require cabling and

power. Best practices dictate that cabling be enclosed in tamper-resistant metal conduit. Due to high costs of installing conduit, many facilities install wiring in cable trays located above false ceilings and in walls. If installation above ceilings or in walls is not possible, wiring must be run within tamper-resistant metal conduit that is attached securely to the walls with metal brackets. Additionally, the further away sensors are from the alarm panel, the more expensive the installation will be.

One way to size your system is to compare your system objectives against an ordered list of potential configurations. Six potential configurations are listed below, in order from least secure to most secure.

1. A few motion sensors located in the main hallways
2. Configuration #1, plus magnetic switches on all exterior doors
3. Configuration #2, plus motion sensors in rooms with valuable items that are easy to resell (computer lab, chemistry lab, band hall, weight room) or that are targets for vandalism, such as a gym or a principal's office
4. Configuration #3, plus motion sensors in every classroom
5. Configuration #4, plus magnetic switches on windows that can be opened
6. Configuration #4, plus glass break sensors near any significant bank of windows. (Note: Glass break sensors are not frequently applied in schools, though their use in schools where broken windows are a common problem might be appropriate.)

The 3rd configuration is probably the most cost-effective for the majority of schools and their security objectives. See Figure 6.3 for an example of this approach implemented within a school. While most individual classrooms are not alarmed, any room with more than the average computer VCR or TV would be. If a perpetrator broke into an unalarmed classroom, they would likely be quickly detected as soon as they stepped into a hallway.

Installation and protection of sensors

Student height is an important consideration when installing sensors. In an elementary or middle school, individual sensors can be installed at the manufacturer's optimal recommended height, which is usually near 7-1/2 or 8 feet. However, sensors installed at 8' or lower at high schools are easily knocked or hit by students (see Figure 6.4). If ceiling height will allow it, it is advisable to install these sensors at a height equal to or greater than 9 feet. While the sensor will not operate as optimally as it was designed for, the performance is degraded by a very small percentage, specifically in its coverage. Remembering this when choosing a site for installation can allow for the full compensation of this slight performance drop (see Figure 6.5).

If low ceilings prevent a higher installation of intrusion sensors, then it helps to place sensors

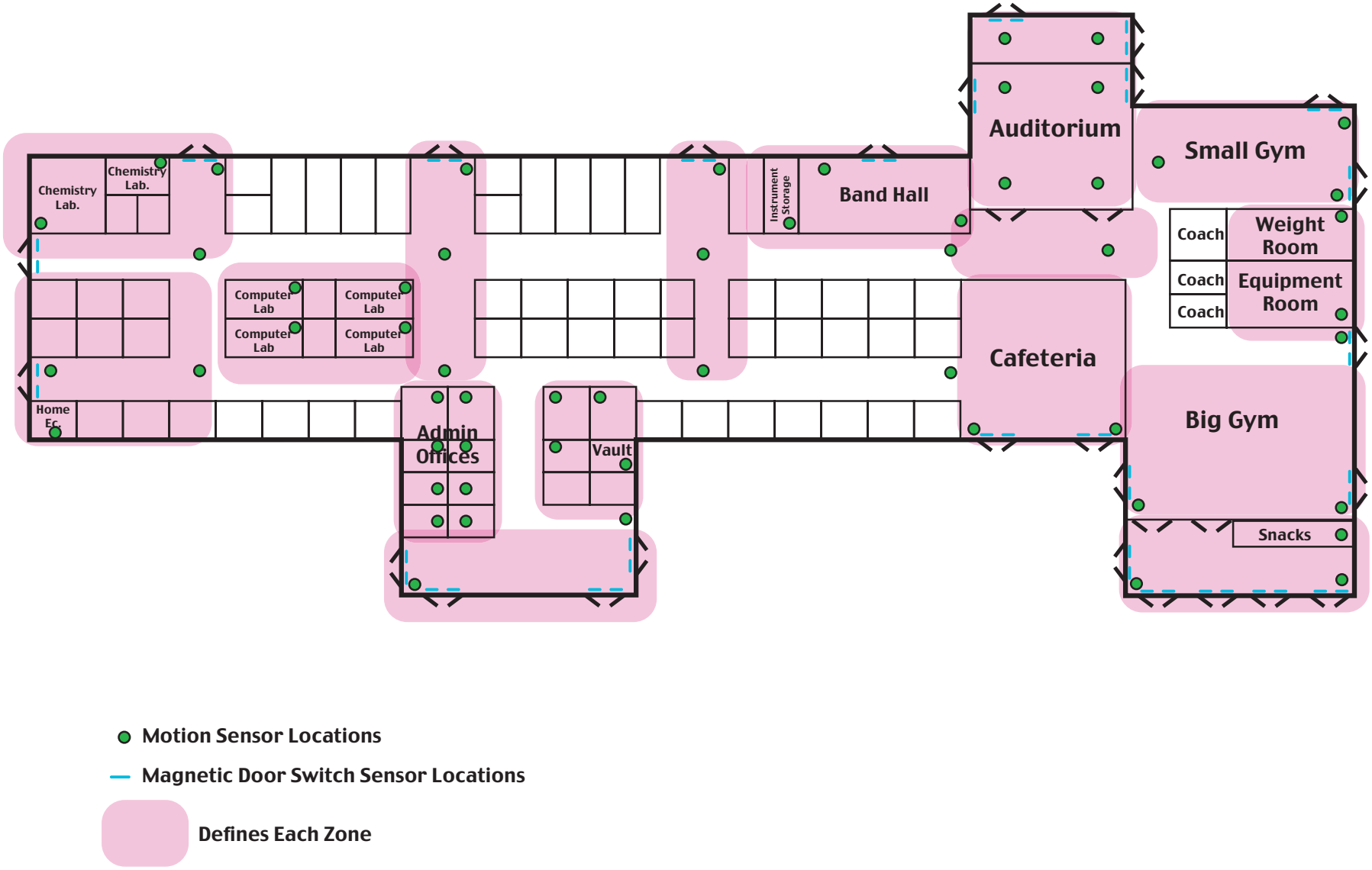


Figure 6.3 This is an example of a sensor design for a typical school. Note the 15 zones that will help responders determine the most recent location of a perpetrator.

Figure 6.4 ***While 8' is the recommended height for installation of most motion sensors, this is usually inappropriate for high schools where many students are well over 6' tall and can easily vandalize them. Note the sloppy installation of sensor wiring in this school hallway; don't let your installer get away with such vulnerable (as well as unattractive) work.***

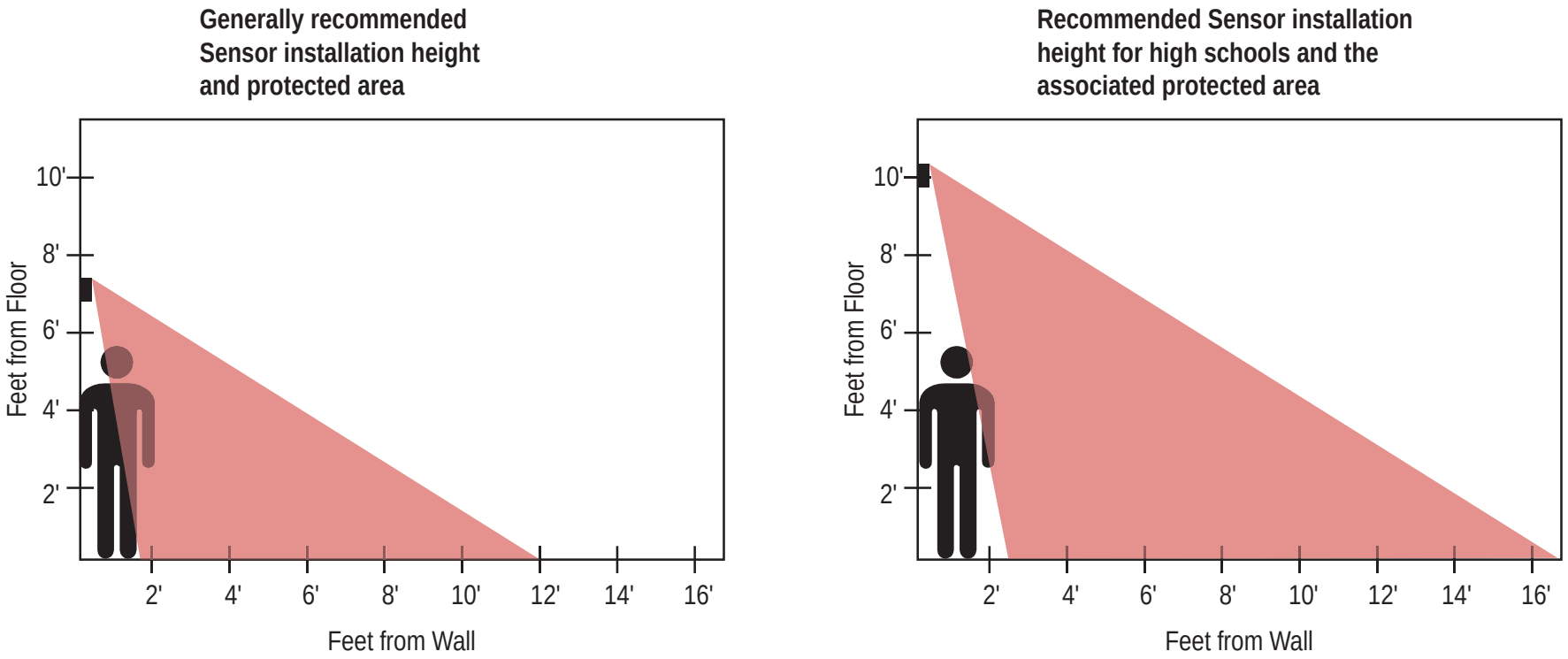


Figure 6.5 ***While installing a motion sensor higher than recommended by the manufacturer can change the protected area (detection zone), if the installer is aware of this change, compensations can be made.***

such that they are more awkward to reach or less likely to be noticed. Right up against an exit sign or in a corner are both examples of areas less prone to be bothered. Some sensors allow for the user to determine and adjust the angle of coverage, thereby compensating for the higher-than-recommended installation. There are also intrusion sensors on the market that are designed specifically for being located at heights greater than 9 feet.

Alarm control panels

An alarm control panel is a gathering point for all sensor data. Most alarm panels also provide a power source for the installed sensors. The cost of a panel is driven in part by the number of zones it accommodates. Typical panels handle between 8 and 32 different zones. Each zone is defined by the input of several sensors located near each other and provides the response team with information as to where in a building the intruder may be. If all the sensors from an entire building feed into one zone, there will be very little information as to the location of an intruder if a detection occurs. Multiple buildings may dictate multiple panels.

When an alarm occurs, a dial-up modem in the panel automatically dials a pre-set number to an alarm monitoring company or police station. A voice modem with a pre-recorded message could also be connected to the alarm panel. When the phone call is answered, the modem delivers a pre-recorded message, giving the name and location of the facility, along with the zone number in which an alarm has occurred. Ideally, the alarm panel should have its own dedicated phone line. The phone line should be protected so that it is difficult to cut. A cell phone could be used as a backup to a land line.

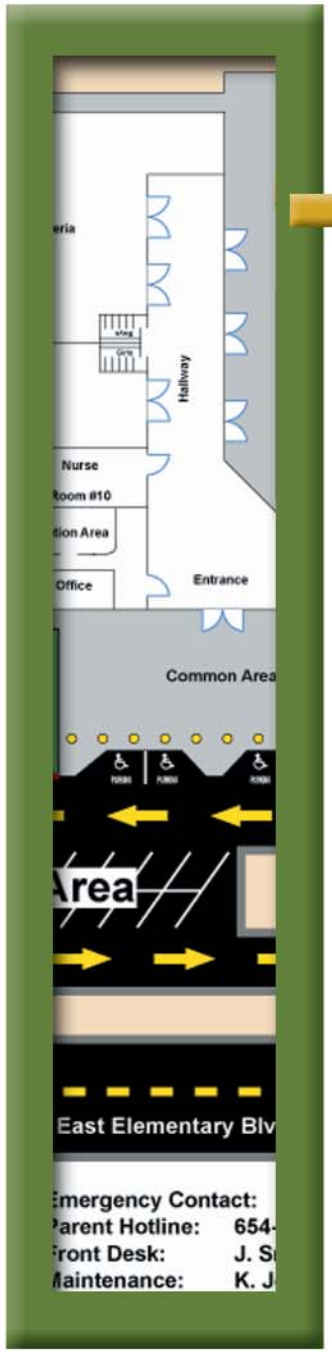
Control panels need to have battery backup as power may be lost occasionally. Most control panels are installed in an electrical closet or other locked utility room where they are protected from vandalism.

Each control panel will have one or more key pads that are used to arm the system at night and to disarm the system in the morning. Key pads should be located where they are not accessible by students, such as in the front office or inside a locked closet near a frequently used entrance. Most key pads allow “pass codes” – number combinations consisting of three or more digits. It is important to keep the codes secure and shared only among a very few trusted individuals.

Many key pads allow for a user to enter a duress code that will notify the monitoring organization that someone is in trouble, such as being held against their will as a hostage or being forced to turn off the alarm. The duress signal is usually an actual pass code, except that it is entered backwards. The duress signal will still disarm the intrusion detection system, but will also notify authorities of the duress condition.

References

1. Adams, D. “Operational tips for improving intrusion detection systems performance.” SAND96-0468C 1996;1-4.
2. Barnard, R.L. *Intrusion Detection Systems*, 2nd ed. Stoneham, MA: Butterworth Publishers, 1988; 147, 217.
3. Cumming, N. *Security*, 2nd ed. Boston: Butterworth-Heinemann, 1992; 115-171.
4. Garcia, M.L. 2001. The Design and Evaluation of Physical Protection Systems. Boston: Butterworth-Heinemann; 87-110.
5. Rodriguez, J., Dry, B., and Matter, J. “Interior Intrusion Detection Systems.” SAND91-0948 1991; 1-114.



Chapter VII
Emergency Management and Planning

Schools should be prepared for emergency situations, although they occur very infrequently, and a complete security program will include protective measures for some emergencies. An emergency is any situation in which the health or life of a student or staff member is in imminent danger, or in which part of the school can be destroyed or rendered unusable. A list of possible emergency situations could include:

1. Severe weather or natural disasters (fires, tornadoes, hurricanes, earthquakes, etc.)
2. A firearm known to be on campus
3. A severe vehicular accident at school or during a school-sponsored event
4. An extremely ill student or employee (i.e. seizure, stroke, heart attack, etc.)
5. A gas line leak or hazardous spill on or near campus
6. Bomb threats
7. Suicide or hostage situations
8. Shooting, stabbing, or sexual assault on campus
9. Local emergencies requiring residents to seek temporary shelter at the school

In the author's opinion it is impossible to fully prepare and protect against such a wide range of emergencies. Still, it is important to develop a working crisis management plan, and much has been written on the subject. This chapter will briefly discuss a few topics and recommendations particularly important for schools, including recommendations on emergency plans, duress alarms, and information and communication during emergencies. Administrators needing further information should refer to an extensive guide published for schools by the U.S. Department of Education, titled *"Practical Information on Crisis Planning: A Guide for Schools and Communities"*. The guide can be found on the department's website at www.ed.gov/emergencyplan. It is highly recommended that administrators follow this or similar guides when developing emergency management plans.

7.1 Recommendations on emergency management plans

An updated, workable emergency management plan is very important in schools. A simple but flexible plan is a valuable enhancement to a school security program. These plans help people react quickly and reasonably to emergencies, and know whom and where to receive direction from. This section will discuss several recommendations for emergency plans in schools.

A 200-page crisis management plan covering every possible scenario is not necessarily better than a simple and flexible 10-page plan. Few administrators, and even fewer staff members, will actually have the time or motivation to read such a plan, and even fewer will remember its contents during an emergency. Some questions that should be addressed in the plan are:

1. What is the chain of command during different types of emergencies?
2. What are the appropriate actions to take for a plausible set of emergencies?
3. What responders (administrators, fire, police, and so forth) should be called first, by whom, from where, and how?
4. If students are to be relocated in a given emergency, where is the assembly point and how do they get there?
5. What type of statement should be made to the press and by whom?
6. Where should emergency responders (fire, police, etc.) establish headquarters when they arrive on the scene?
7. What forms of communication are available to staff and responders (radio, phone, PA system, duress alarms, etc)

Recommendations to help schools prepare for emergencies

The following recommendations are important measures designed to help schools implement their emergency plans more effectively.

1. Provide cell phones (or long-range, two-way radios) for bus drivers, and prepare simple sketches their routes. The sketches can be quickly provided to police in the event of an emergency affecting one or more school buses.
2. Install emergency lighting in rooms having no source of light (i.e., no windows) during a power outage, and provide staff with powerful portable flashlights.
3. Create laminated posters displaying pertinent information and protocol in every classroom, lab, gym, and office area. This is a simple way to implement an effective crisis plan. The names and phone numbers of in-charge individuals can be easily changed each year. It is helpful to include a diagram of the campus and buildings. Such diagrams are popular to use in schools to illustrate fire exits, but become a more effective tool when combined with general emergency protocol (see Figure 7.1).
4. Every middle school and high school should have at least one armed SRO (School Resource Officer) on-site who is trained to respond to a dangerous situation. Every elementary school should be able to summon an officer quickly from nearby.
5. Consider a phone system which records all calls to handle threatening telephone calls to the school. Each time a call is made to the school, a recording announces: "Thank you for calling Main Street High School. This call will be recorded for quality purposes." Most wrongdoers do not like their voice being recorded, even if they attempt to disguise their voice (see Figure 7.2).

Environmental emergencies and accidents

The following recommended protective measures are designed to help schools mitigate (or even prevent) the effects of an environmental disaster or accident. Some of these situations could include a chemical or biological attack, hazardous waste spill (i.e., from an overturned tractor trailer), or contaminated drinking water.

1. Ensure that access to the school's fresh air intake and water source is inaccessible by the general public. This measure can prevent a perpetrator from introducing biological or chemical hazards into the school's air or water system (see Figure 7.3).
2. If there are factories, storage plants, or major highways located near a school, meet with the management of these facilities and/or the highway department to discuss possible disasters, their ramifications, their likely solutions, the best medical response, etc. Having a known contact and phone number to call at the state or local level can expedite a school's decision as to the best way of handling a serious environmental hazard.
3. Learn the best steps to take for the most-likely events in your area. For example, do not assume that the HVAC system should be turned off in

the event of a near-by chemical spill or other environmental issue. It is possible that once dangerous vapors have already entered a building, operating the HVAC system may clear away any noxious fumes from rooms, but this depends on the actual event.

4. If risk of environmental emergencies is high, consider installing a small outdoor weather station with airspeed and direction indicators, so this information can be checked and reported if an environmental emergency does occur.

7.2 Duress alarms

Some emergencies, such as a hostage situation or armed robbery, are constrained by the need for extreme urgency, covertness or discretion (perhaps because of an intimidating situation). In these cases, it may not be possible to summon help through normal communication methods (i.e., phone or radio, yelling and shouting, sending someone to find help, etc) for fear of reprisal or the time required to call for help. A duress alarm is recommended for these situations. A duress alarm sends an immediate distress signal to a predetermined location(s) at the push of a button.

Modern duress alarms vary widely in capabilities and price. The three general categories of duress alarm are:

1. Panic alarms – an alarm switch mounted in a fixed location;
2. Identification alarms – a portable or fixed switch that identifies the owner of the device when initiated; and
3. Identification/location alarms – a portable device that identifies, locates, and sometimes tracks the person who activated the duress alarm.

A possible fourth category is cellular telephones. While not as discrete or as automatic as the above alarm categories, a cellular telephone is highly recommended equipment for principals and security personnel.

Panic alarms

Panic alarms are simple, effective and affordable for schools (see Figure 7.4). They usually consist of strategically located buttons that are connected to a phone modem and a dedicated phone line. Such a system can be installed for a few hundred dollars per panic button, by a local electrician, plus the monthly cost of the phone line. Figures 7.5 and 7.6 show one conceptual panic alarm design.

When initiated, a prerecorded message (such as, *"Main Street Middle School is experiencing a crisis situation. Please respond ASAP. We are located at 213 Main Street, just south of East Street. Our phone number is 510-3997"*) specifying the school, its location, and the alarm status is sent via wiring, to several locations, such as the police department or the district security office and displayed on a console. The console would show the location of the activated alarm, but does not say who initiated it. (After receiving a duress signal from a classroom, the front office could activate the room's intercom

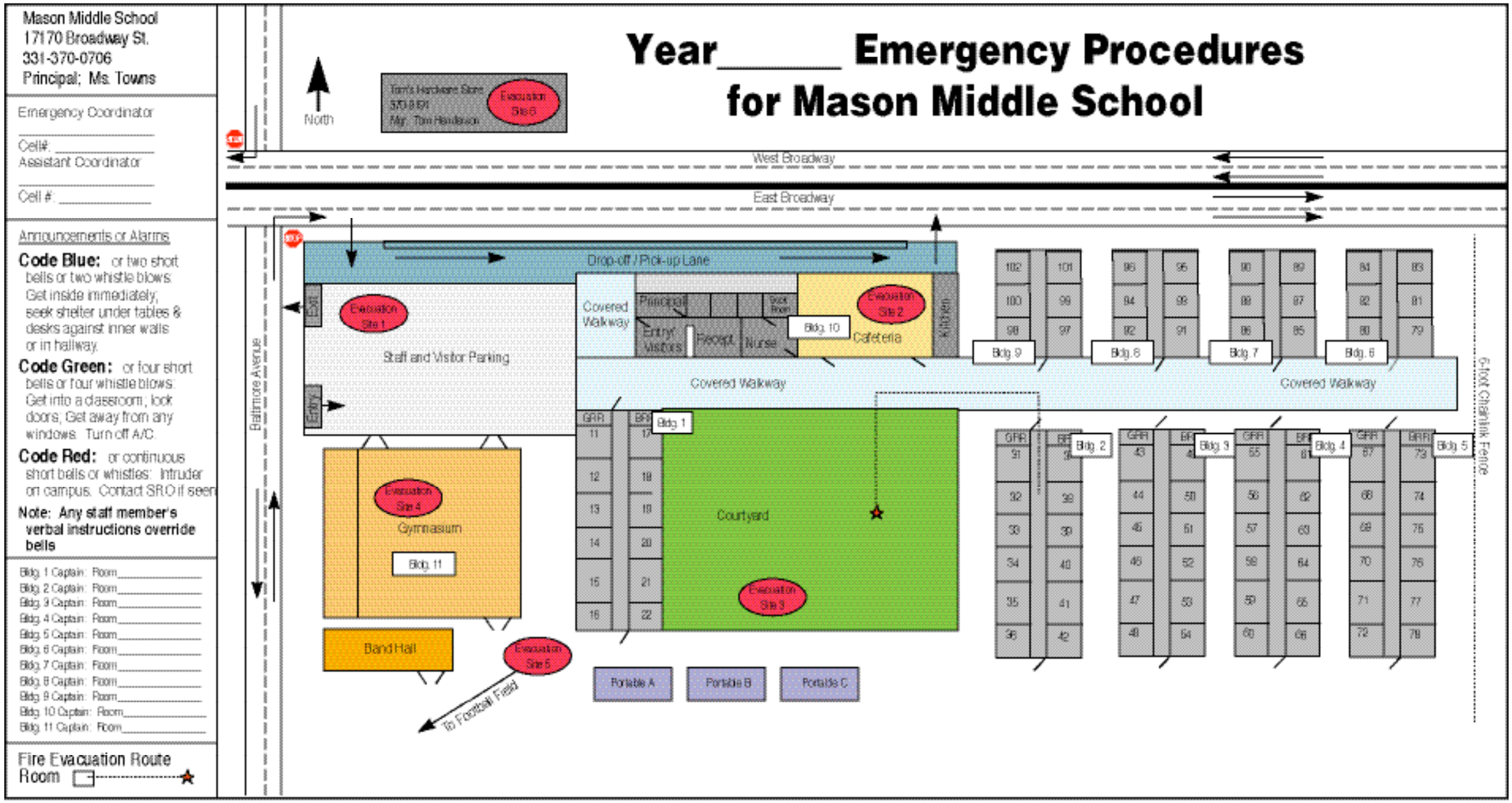


Figure 7.1 ***This is an example of an Emergency Poster that could be posted in all classrooms, student areas, and offices. Notice that changes each year is a "blank" underline – the poster is intended to be laminated and is then reusable by changing the infor mation in the blanks by hand with a marker or printed tape each year. This poster plus staff training, can create an excellent tool to present evacuation plans as well as code definitions.***

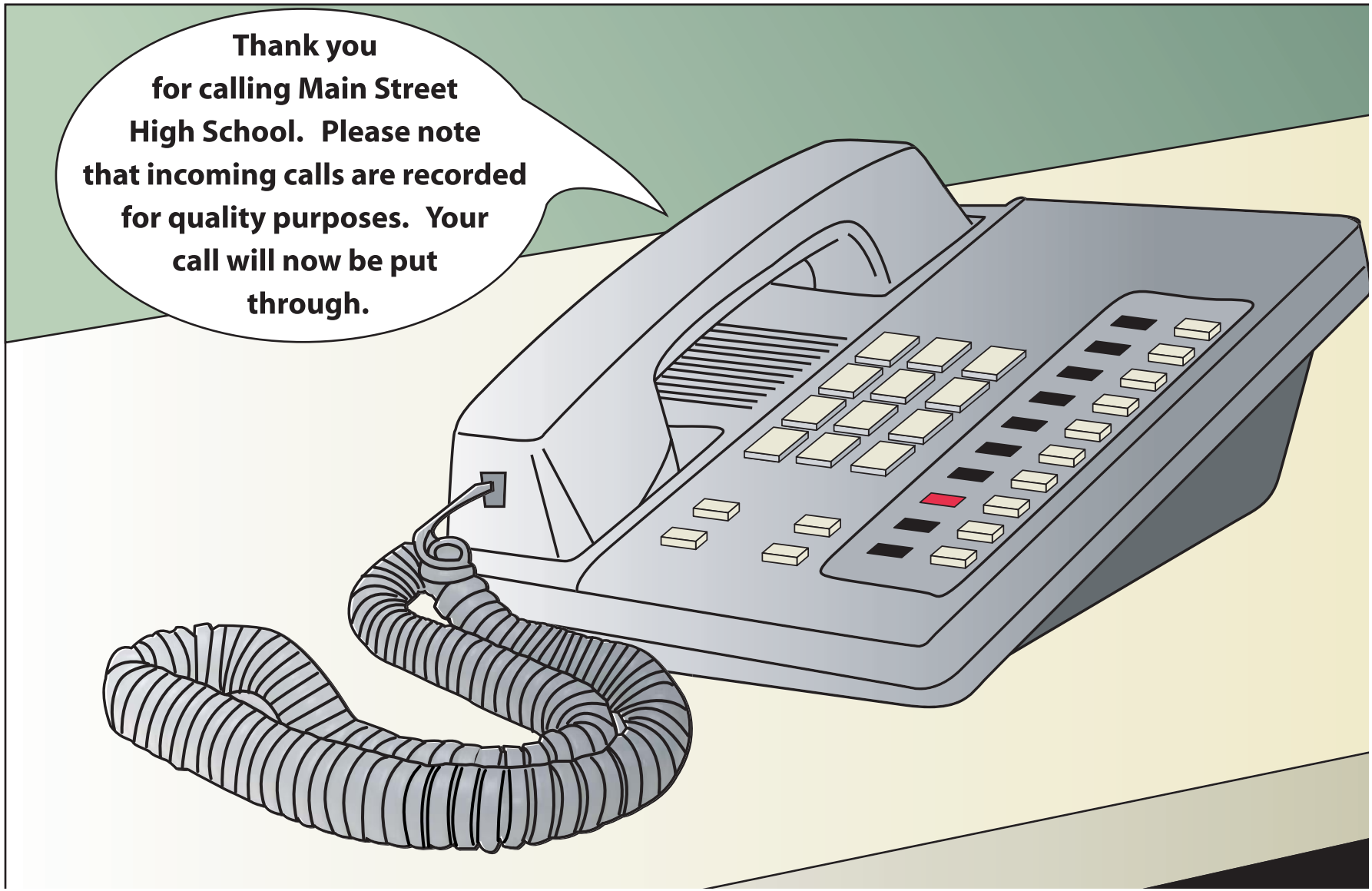


Figure 7.2 One possible deterrence against threatening phone calls is a phone system set up to initially greet callers with a notice regarding the recording of all calls.

Figure 7.3 Where is the air intake/handler for your school building? It is preferable that the unit be located on the school roof top or an area of the campus inaccessible except to authorized personnel.

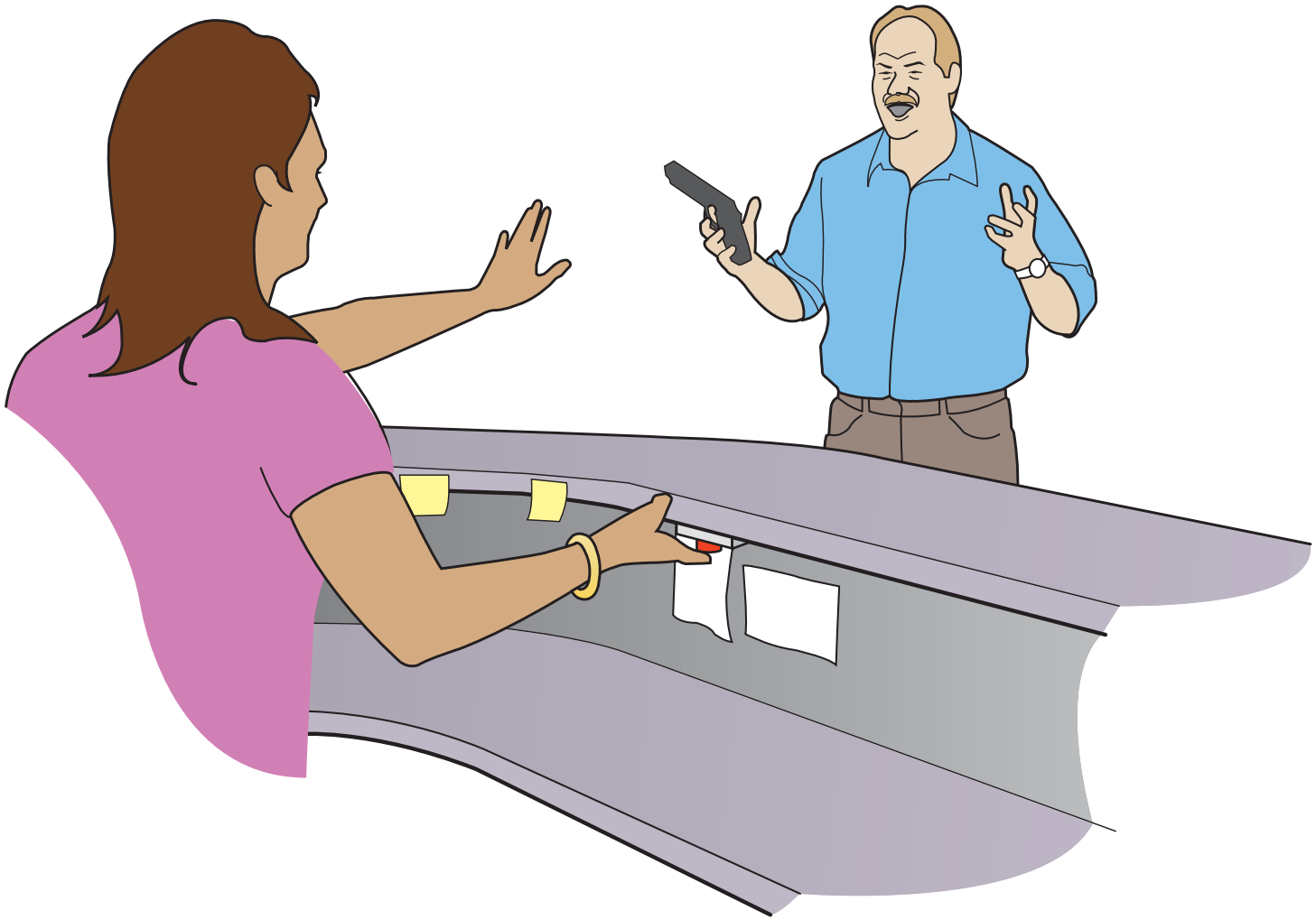


Figure 7.4 ***This illustration shows a simple duress system for a school's front office. Every public and private school needs some method of contacting the police or other emergency response quickly and automatically in the event of a true emergency.***

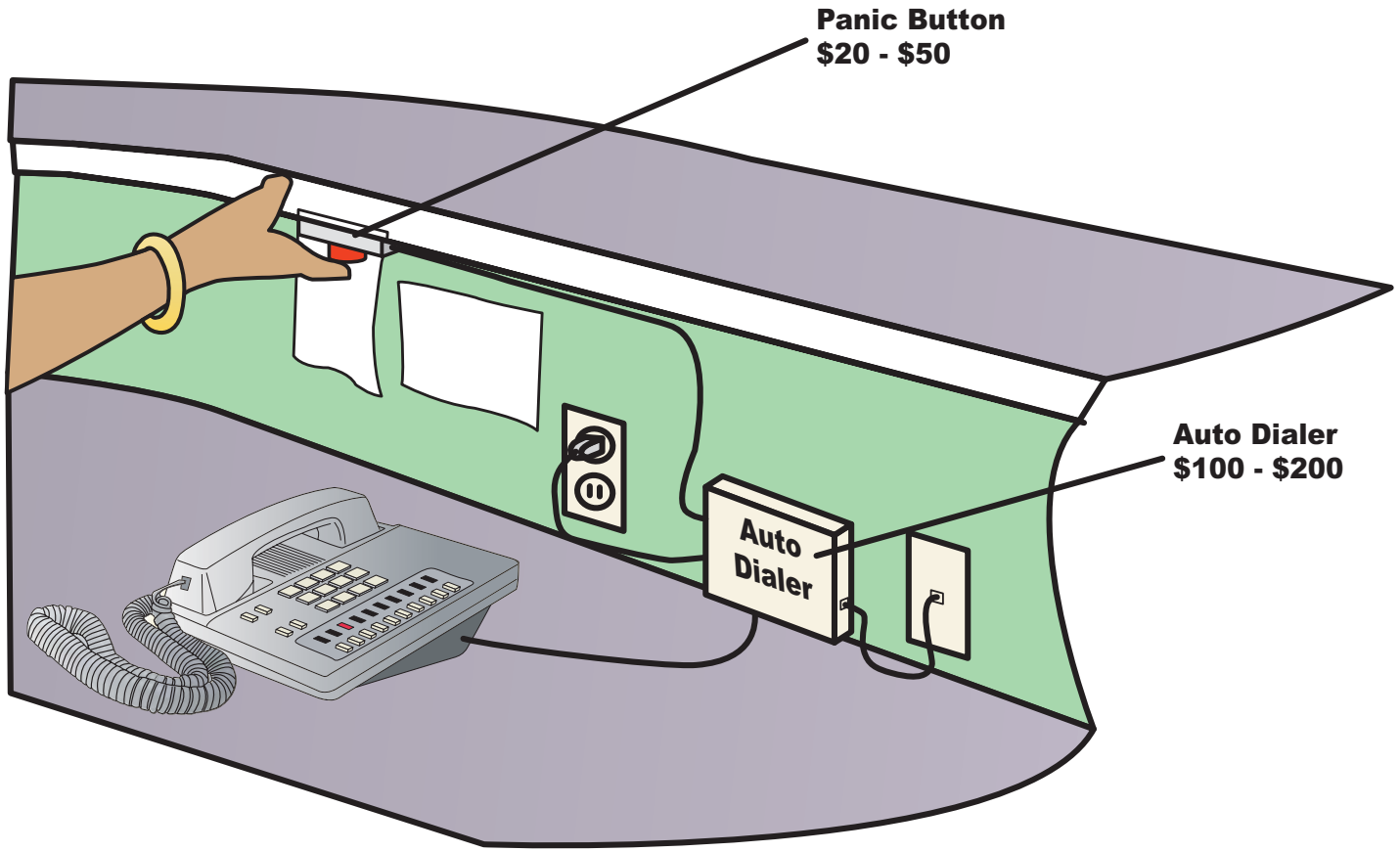


Figure 7.5 ***This illustration shows the simplicity of creating your own panic alarm system. These components should be available through an electronic parts store. You will need to record your own emergency message onto the auto dialer. The entire system cost, including installation, should be less than $500, though a dedicated phone line will be an on-going expense.***

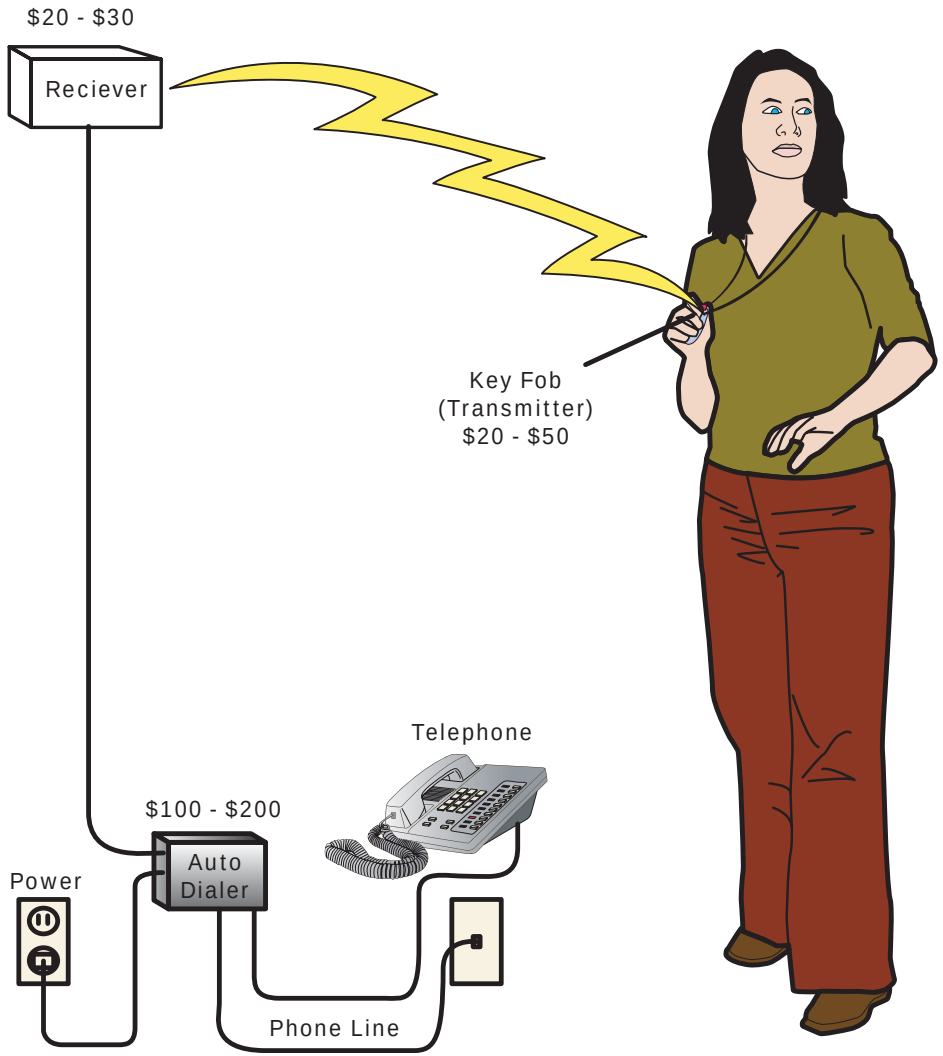


Figure 7.6 While this illustration shows how simple it is to put together a wireless duress panic button system, it must be remembered that there must usually be line-of-sight between the wireless keyfob and the receiver.

and listen to what is happening. A school can even choose code phrases or questions ahead of time as part of their crisis plan that the front office and employee under duress would exchange that have previously agreed upon meanings.)

Panic alarms have some weaknesses. First, they can not identify the person using it, although they do report the location of the alarm. Second, they may not be readily available in a duress situation if located across the room from the teacher's current location, or if accidentally blocked by furniture and posters. Third, thoughtless students can trigger numerous nuisance alarms, though this can be offset by hiding the pushbutton or requiring a PIN before use. (A PIN is not recommended for schools because of the potential liability of a student attempting unsuccessfully to summon help in a threatening situation.)

Identification alarms

An identification alarm uses a pager-like device with a built-in panic button and is worn or carried by school personnel. When initiated, the alarm signal is received by the closest installed wireless sensing unit that transmits the signal to the alarm console. The console would display a code or other information identifying the staff member. This system does not usually identify the alarm's location, other than the zone (or location) of the sensing unit. Increasing the number of zones requires more wireless sensing units, which increases the cost and complexity. Unless there is a clear line-of-sight between the pager and the receiving unit, obstructions can attenuate the signal, decreasing the chances of receiving it and identifying an individual under duress.

Identification alarms can incorporate a two-way radio into the pager that allows communication between the console operator and person under duress, but this larger pager is more awkward to wear. It is possible for the duress system to 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.

Identification/location alarms

Identification/location alarms can identify, locate and often track the person who activated the duress alarm. Again, the alarm is activated via a device (sometimes referred to as a key fob) worn or carried by the person under duress. An extensive wireless infrastructure begins tracking signals from the pager device (see Figures 7.7 and 7.8) and displays identity and position information on a console or map-like display. This type of system is expensive initially and requires some manpower to maintain and operate.

Costs for commercially available duress alarm systems vary widely. Telephone calls made in the fall of 2004 to companies specifically targeting schools in their marketing strategies produced a wide range of estimated costs. School layout, building age, and school size all can greatly affect the final price. For estimation purposes, administrators can plan on systems costing between

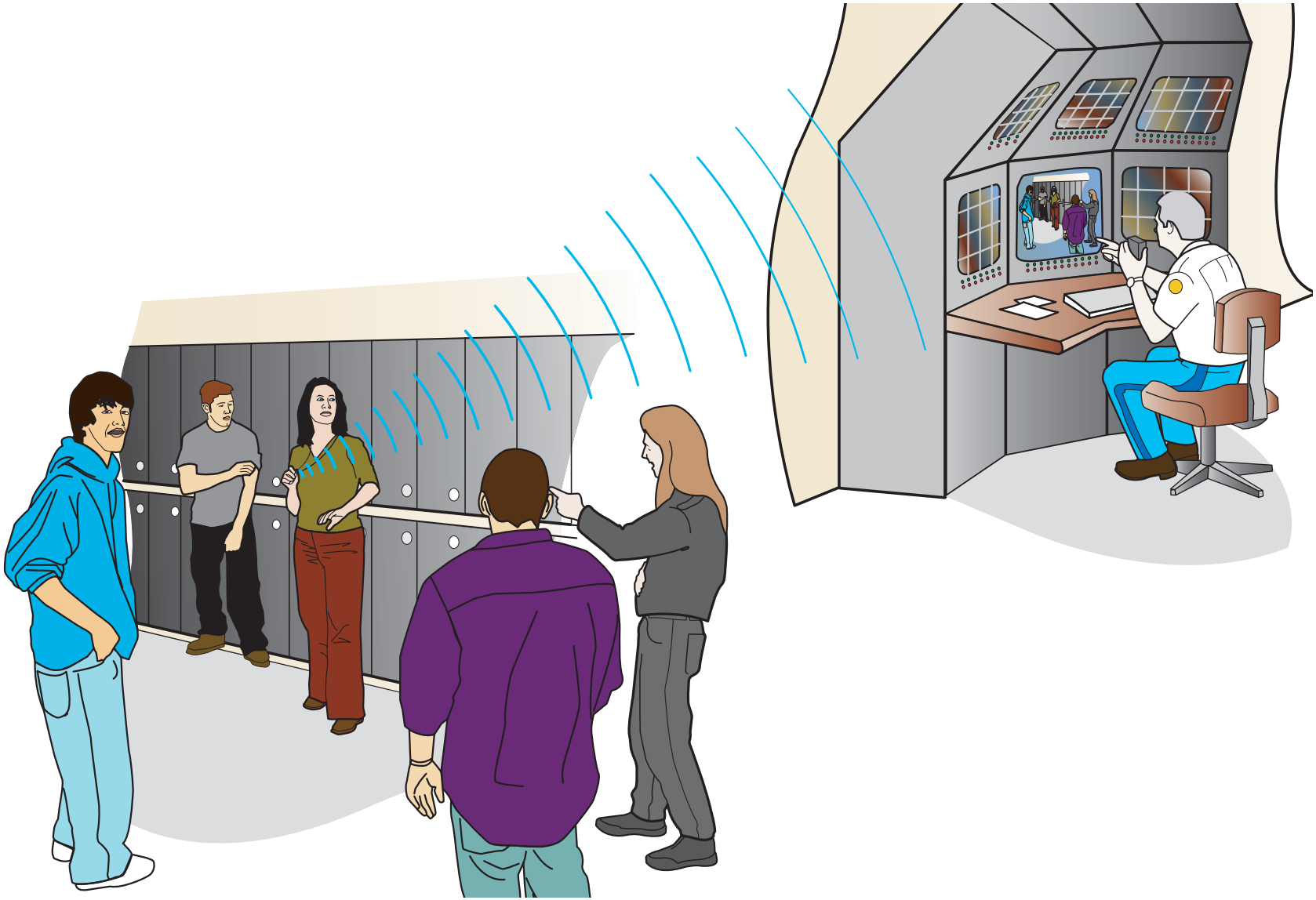


Figure 7.7 ***A wireless identification/location duress alarm allows a facility to determine from where and from whom a duress signal has been sent. Unfortunately, this sophisticated technology is more expensive than most schools can afford plus generally requires much more manpower to operate and maintain.***

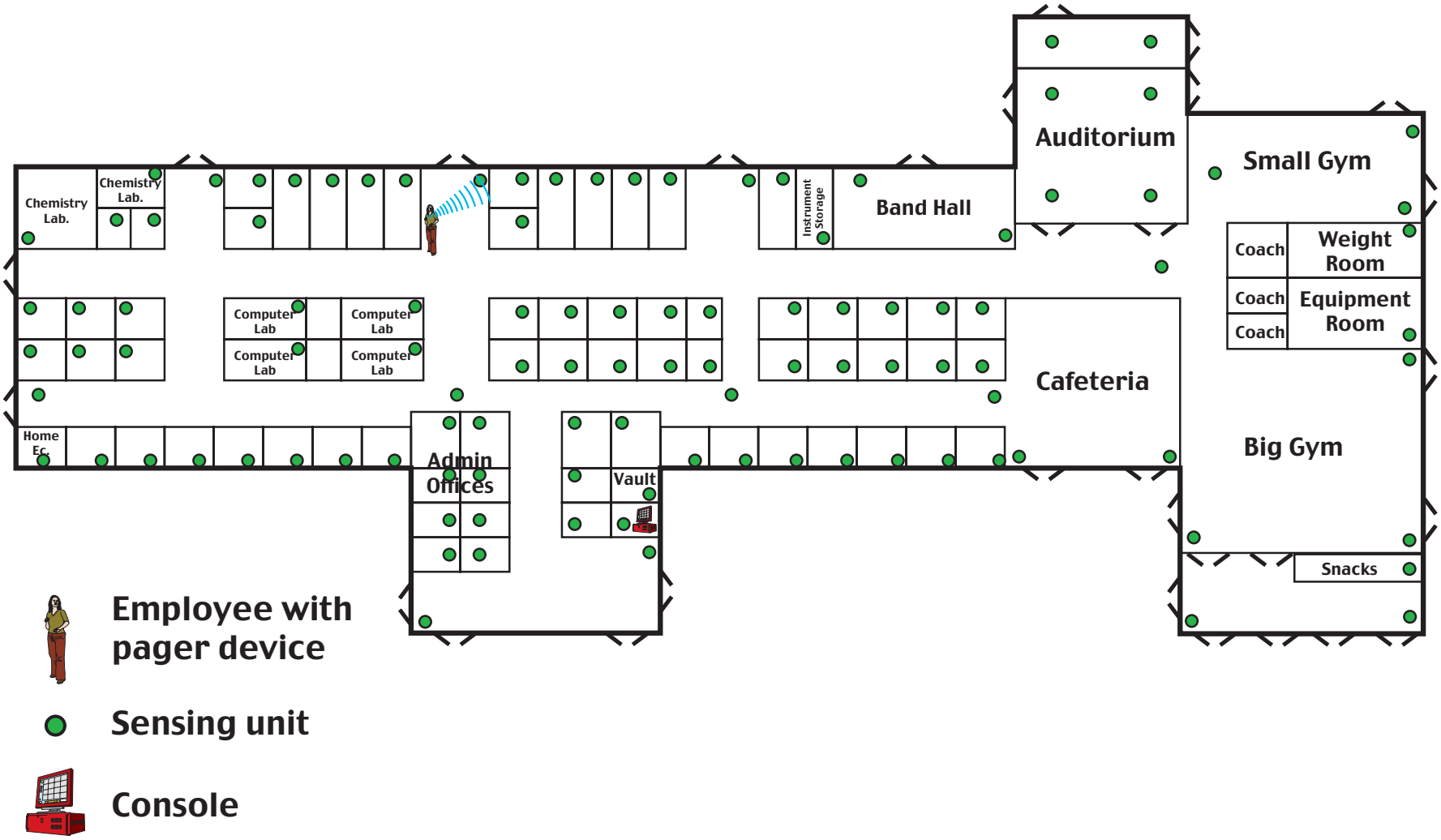


Figure 7.8 This is one example of how receivers for RF (radio frequency) duress alarms would need to be installed throughout a school for an identification/location type duress system.

$150 to $1000 per teacher or employee having duress capability. While many schools cannot afford the more sophisticated duress systems, they should provide the following as a minimum for their staff:

- A panic button-type duress alarm installed in the front office and in similar locations that warrant this type of backup support.
- A method for all classroom teachers to summon immediate help in the event of an emergency (i.e., through an intercom system, a telephone in each room, or a cell phone).

7.3 Information and communication during emergencies

Credible information, and the ability to communicate it with staff, students, the community and emergency responders, is vital in all emergencies. The following recommendations are designed to help schools maintain reliable information and communication during emergencies.

1. Implement an anonymous student hot-line or Crime-Stop0pers type program can encourage students to report malevolent actions that a friend or acquaintance has done or is planning.
2. Encourage parents to come in and speak with the school staff or even the SRO (School Resource Officer) when they suspect the development of a potential security incident with their own child or with one of their child's friends (i.e., plans to bring a weapon to school or harm others)
3. Invite residents living next to your school to come in once a year and voice their security concerns regarding the students or the campus. Let them know whom to call if they notice suspicious activity. A few "nosy neighbors" can be excellent allies and provide valuable information for some types of problems. Limited explanations of the school's alarm system, audio warnings, and expected response force can make neighbors feel much more comfortable about what is going on at the school.
4. Set up a telephone number that parents can call to hear an updated recording during an emergency. This could include situations such as icy roads, tornado alerts, gas leaks near the school, a shooting that has been picked up by the media already. These events tend to leave parents wondering whether they should rush to the school to pick up their children, meet them at an alternative gathering site, or expect them to come home early on the buses. A website that also includes this same information can be very useful in some communities (see Figure 7.9).
5. Consider purchasing two-way radios, which are important assets during any emergency. Most schools emergency situations requiring immediate communication with the principal, a teacher on duty, school nurse, front office or the SRO. Each time an administrator leaves the front office, a two-way radio should accompany him. It is good practice for teachers on playground, parking lot, or cafeteria duty to

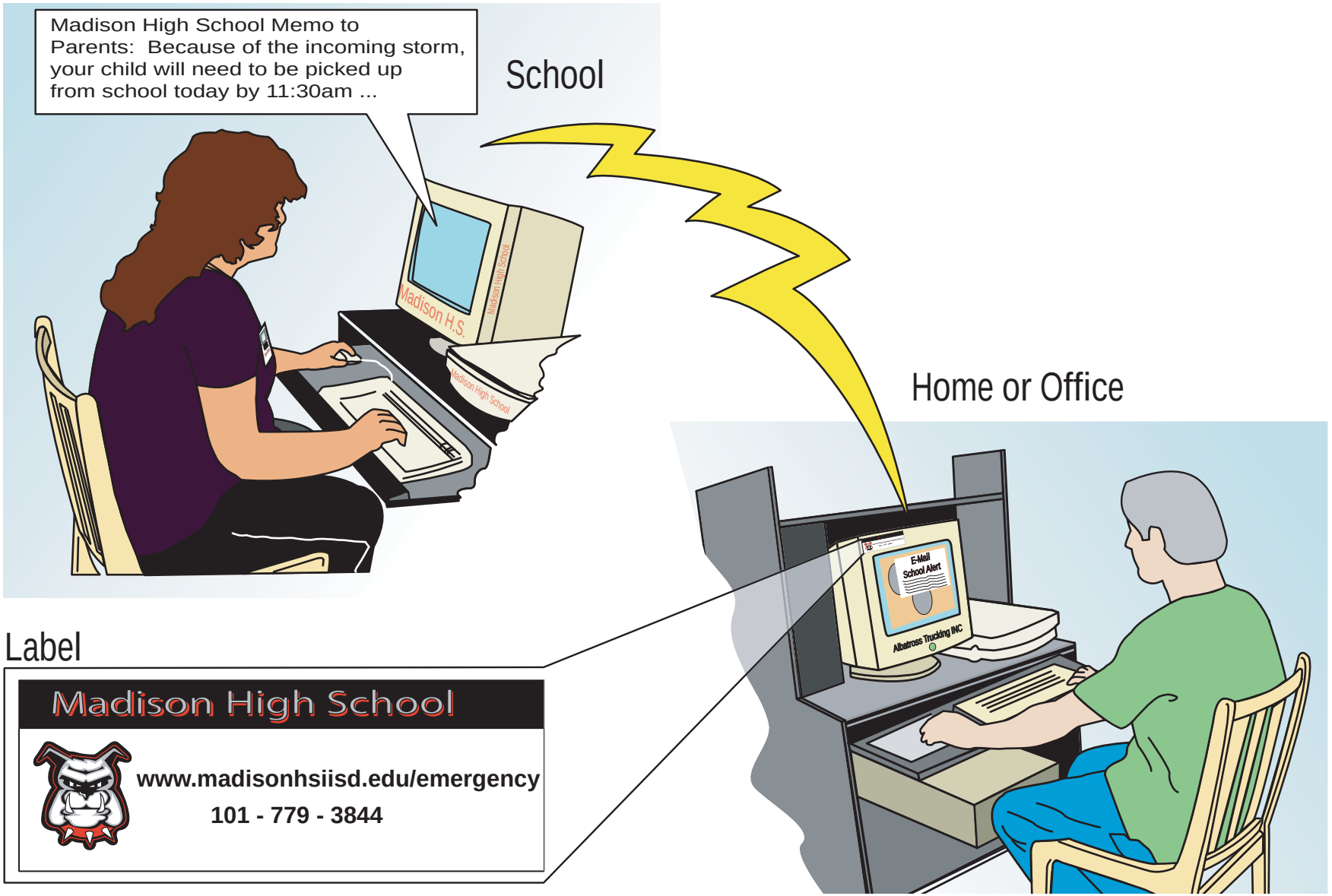


Figure 7.9 ***Many communities will be appreciative of a school website where they can check for emergency messages in the event of a crisis. Mass e-mailing systems can also be effective. Sending home stickers with the web address for parent to affix to their work and home computers, along with an emergency telephone number, can greatly assist a school or school district in notifying parents quickly.***

check out a two-way radio for the duration of their oversight duties.

6. Typical school campuses will not be able to use the ubiquitous $25 walkie-talkies that are available today. In general, these low-cost radios do not have the power to transmit through several school walls. School walls are typically built of cinder block or concrete reinforced with rebar (– it is normally the rebar that attenuates the signal). Districts can expect to pay between $300 and $500 per two-way radio, with features such as multiple channels, a low-battery indicator, and rechargeable batteries. Test the radios you are considering purchasing, in multiple locations on campus, before purchasing them, to ensure adequate coverage.

7. Number classrooms and offices on the exterior of the building, if necessary, to make it easier for emergency personnel to respond quickly to the correct location on campus (see Figure 7.10).

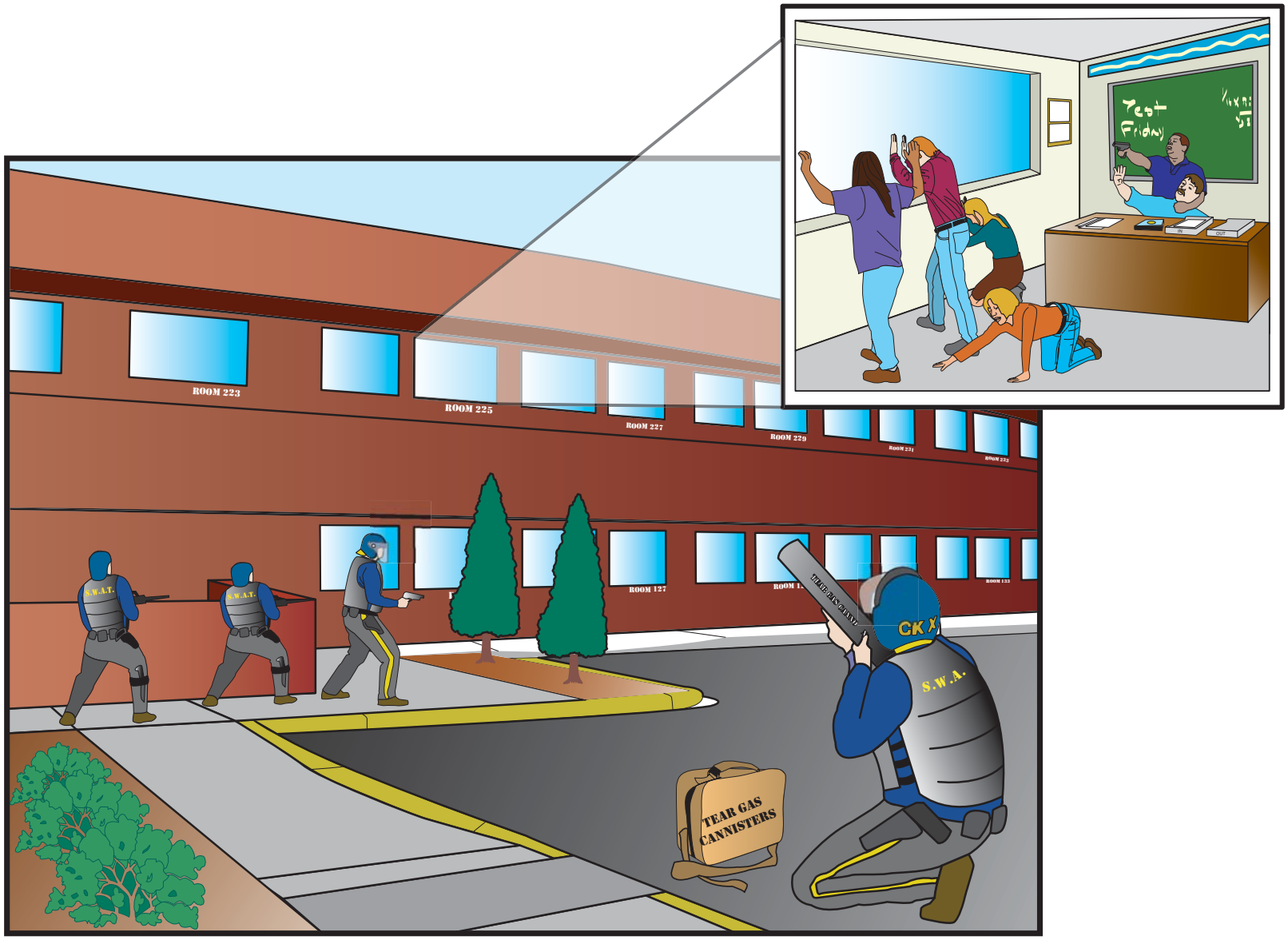


Figure 7.10 Simply marking classroom numbers on the outside of a school building can enhance the early effectiveness of response teams in some situations. Even cardboard signs inside the corner of a window can possibly save a few precious seconds. Local response teams should be provided with up-to-date school layouts at the beginning of each school year.

Chapter VIII
Appendices

Appendix A. Sample School Security Assessment Questionnaires

One of the more frequent requests the authors have received over the past ten years is for a generic security survey form. Additionally, the process outlined in Section 2.1 discussed collecting stakeholder concerns regarding school security as part of the process of characterizing the school. Accordingly, three sample questionnaires (one for students, one for teachers, and one for the school administrators and security staff) are given below for schools utilizing the method presented in Section 2.1. Only a subset of the students and the teachers are needed to complete them. An excellent group of students for this exercise might be the Student Council, as these students may take the task more seriously than other students.

It is usually helpful, though expensive, to have an outside security consultant conduct a more thorough, formal assessment. They are trained to identify security vulnerabilities and will usually discover items school personnel may have overlooked. Enlisting the help of a consultant may not be possible in many cases. Therefore, the questionnaires are also intended to help schools identify and prioritize security incidents of concern, if they are not following the detailed process outlined in Section 2.1 or enlisting the help of a consultant.

If this is the case, the accumulated responses should be reviewed and used as input data for the process outlined in Sections 2.2 and 2.3. Of course, the questionnaires are not all-inclusive of every possible problem or area for consideration. They create a foundation for assessing where potential security problems on a school's campus

may exist, but do not constitute a comprehensive or professional assessment.

One of the most frequent requests that the author has received over the past ten years is for a generic security survey format. With all of the negative attention that school security incidents are receiving these days, many administrators and security personnel are busy trying to determine whether they are fully aware of all the possible "security holes" within their schools. Nobody wants to find themselves in the position where their lack of foresight allowed harm to befall upon a student or staff member, especially if it could have been avoided.

Unfortunately, there is no one-size-fits-all security survey. If there's anything that has been learned by the author after visiting many, many schools, it's that no two schools are alike. Not only are schools different, but their security problems are different and come in different packages from different sources and all will be handled differently with different consequences and different changes to the program. This is so because schools and security problems are all made up of people, and people are so different.

While it is usually helpful, though expensive, to have an outside consultant visit a school, and they can usually notice a few things on every campus that perhaps the school personnel might have overlooked, it would be very unusual for that consultant to be able to pinpoint all the hotspots and determine the optimal solution for each school, because they can't really know the personality or flavor of this small community of people. And they certainly can't second-guess who on the campus is going to try something next and what that might be.

Surely, the people who know a campus the best are the people who work there and walk the halls every day. So, to at least get a school started on a more formal assessment of their environment, enclosed are three different questionnaires – one for students, one for teachers, and one for the school administrators and security staff. Only a subset of the students and the teachers will probably be needed to fill these out. An excellent group of students to request this support from would be the Student Council, as it is hopeful that these students may take this task more seriously than other students.

These questionnaires should serve as a strong foundation for assessing where the potential for problems on a school's campus may exist. The accumulation of the responses that are gathered should help lead the security team in the direction they need to go. Almost all of the issues covered in these questionnaires have been covered in the first nine chapters of this document. Of course, these questionnaires are not all inclusive of every possible problem that could arise – they need to be customized and supplemented by knowledgeable staff to fit their own particular school. Copies of the questionnaires may be downloaded from the Sandia website: www.sstar-sandia.org

With the electronic version of these questionnaires, it should be easier for the security team to customize them for their own needs.

Security Questionnaire for STUDENTS
School Name: _____
Grade level: _____ **Date:** _____
[Continue longer answers on a separate sheet of paper]

(1) If you arrive at or leave school when it is dark outside, do you feel safe walking to and from the school building?
Yes [ ] No [ ]
If you answered *No*, please explain any concerns you may have:
_____
_____

(2) If you drive a vehicle to school, do you feel your vehicle is safe in the parking lot? Yes [ ] No [ ]
If you answered *No*, what do you think should be done to make it safer? _____
_____

(3) If you ride a school bus to and from school, do you feel safe on the bus? Yes [ ] No [ ]
If you answered *No*, what would make you feel safe when on the bus? _____
_____

(4) How would you rate the appearance of the exterior of your school? (*The age of the buildings should not necessarily be a factor – clean grounds, lack of weeds, pleasant and well-cared for landscaping, maintenance of buildings, etc. are more important.*) Rate the school on a scale of 1 to 5, with 1 being the least desirable.

Dirty, poorly maintained	1	2	3	4	5	Very clean and well cared for

If you rated your school less than a "4", specify what you feel the particular problems are? _____
_____
_____

(5) How would you rate the interior appearance of your school on a scale of 1 to 5, including halls, classrooms, gym, restrooms, etc?

Dirty, unpleasant	1	2	3	4	5	Very clean and well cared for

If you rated your school less than a "4" above, specify what you feel the problem areas are: _____
_____
_____

(6) How often are teens or other young adults hanging around on school grounds who are not supposed to be there (i.e., if they are not students at your school)?

Constantly	1	2	3	4	5	Almost never

If you answered other than "5" above, describe these people, and how are they able to enter school buildings? _____
_____
_____

(7) Could you name any places on campus where you feel particularly unsafe? (such as in the restroom, in the locker bay area, etc.) _____
_____
_____

(8) If you heard that a student at your school was planning to cause some violence on your campus, would you tell an adult about it? Yes [ ] No [ ]

How would you tell someone about it? *[Check all that apply]*

[ ] I would tell the principal or assistant principal
[ ] I would confide in a teacher I know and trust
[ ] I would speak to one of the school resource officers or guards
[ ] I would use an anonymous telephone Crime-Stoppers Hotline, if available
[ ] I would tell my parents
[ ] I would leave an anonymous note with the front office

(9) How often do you think weapons are brought to school?

Constantly 1 2 3 4 5 Never

If your answer was less than "5", what types of weapons are most common and why do you think students bring them in?

_____

_____

(10) Do you believe that illegal drugs are brought onto campus?

Constantly 1 2 3 4 5 Never

If your answer was other than "5", what types of drugs are most common? _____

_____

What percent of the students do you feel may be using illegal drugs on a regular basis?

1% [ ] 5 – 10% [ ] 21 – 30% [ ]
2 – 4% [ ] 11 – 20% [ ] > 30% [ ]

(11) Do you believe that students bring alcohol onto your campus?

Constantly 1 2 3 4 5 Never

(12) Does your school use dogs for drug searches? Yes [ ] No [ ]

If *Yes*, do you think this cuts down on the amount of drugs brought to school? Yes [ ] No [ ]

Why? _____

_____

If your school does not currently use drug sniffing dogs, do you think bringing in dogs to search lockers and vehicles would help cut down on drugs at your school? Yes [ ] No [ ]

(13) Are there particular groups of students in your school who you feel cause the majority of security-related problems? Yes [ ] No [ ]

If you answered *Yes*, describe these groups: _____

_____

_____

(14) Which of your security concerns would you rate as the most important to the safety of your school, its occupants, and the community?

Most important: _____
Second most important: _____
Third most important: _____

Do you have any other security concerns you would like to mention? _____

_____

_____

_____

_____

_____

Thank you for your time in answering these questions.

Security Questionnaire for TEACHERS
School Name: _____
Date: _____
[Continue longer answers on a separate sheet of paper]

(1) If you arrive at or leave school when it is dark outside, do you feel safe walking to and from your car? Yes [ ] No [ ]
If you answered *No*, please explain your concerns: _____
_____
_____

If you believe the nighttime exterior lighting is inadequate, what improvements do you feel are needed? _____
_____
_____

(2) Do you feel your vehicle is safe in the parking lot?
Yes [ ] No [ ]
If you answered *No*, what could be done to make it safer?
_____
_____

(3) Do you feel that the bus drop-off and pick-up area is safe, both from a traffic perspective as well as from malevolent outsiders or insiders? Yes [ ] No [ ]
Are there enough adults assigned to monitor this area?
Yes [ ] No [ ]
If your response to either question is *No*, what improvements do you recommend? _____
_____
_____

(4) Do teachers have (and use) two-way radios when on bus duty or assigned to oversee a particular part of the campus?
Yes [ ] No [ ]
Do they work properly and transmit adequately from various parts of the campus to the front office?
Yes [ ] No [ ]
If your response to either question is *No*, please explain: _____
_____
_____

(5) Do you feel the exterior/grounds of your school campus are well cared for? Yes [ ] No [ ]
How would you rate the exterior appearance of your school on a scale of 1 to 5? (The age of a school should not necessarily be a factor – clean grounds, lack of weeds, pleasant and well-cared for landscaping, maintenance of buildings, etc. are more important.)

Dirty, poor upkeep	1	2	3	4	5	Very pleasant and inviting

If you rated your school less than a "4", specify what you feel the problems are: _____
_____
_____
_____

(6) Is the interior of your school is well-cared for?
Yes [ ] No [ ]
How would you rate the interior appearance of your school on a scale of 1 to 5?

Dirty, poor maintenance	1	2	3	4	5	Very clean and cared for

If you rated your school less than a "4", specify what you feel the problems are: _____
_____
_____

(7) How difficult is it for visitors to your school to bypass the office and go directly to a classroom or other student area?

Easy, no one watches 1 2 3 4 5 Difficult, visitors always stopped

If you rate your school less than a "4", what do you think would improve this situation? _____

_____

_____

(8) How often do you feel unauthorized non-student persons are in your hallways?

Constantly 1 2 3 4 5 Almost never

If you rate your school less than a "5", how do you think they enter the school building? _____

_____

_____

How many exterior doors (other than the front office) are left unlocked during the school day in your main buildings?

Most or all [ ] Just a few [ ] Only main entry doors [ ]

How frequently are exterior doors propped open during the day by students or teachers?

Frequently [ ] Occasionally [ ] Almost never [ ]

Do you feel this needs to be rectified to keep unauthorized visitors out of your buildings? If yes, please explain:

_____

_____

(9) Are teachers always allowed access to their classroom after hours? Yes [ ] No [ ]

If yes, how do you get in?

I Have a key assigned to me [ ]
The custodial crew lets me in [ ]
I call security to let me in [ ]
Other _____

Do all teachers have an access code to turn on/off the intrusion detection (burglar alarm) systems during off-hours?

Yes [ ] No [ ]

Do you feel safe in the building late in the evening if you are by yourself? Yes [ ] No [ ]

If you believe the nighttime interior lighting is inadequate, what specific improvements are needed?

_____

_____

(10) Do you feel adequately trained in emergency procedures at your school for incidents (such as a hostage situation, violent intruder, gas leak, etc.)? Yes [ ] No [ ]

Do you feel the school's emergency response plan is reasonable?

Yes [ ] No [ ]

If not, in what way(s)? _____

_____

What would make the plan better? _____

_____

_____

(11) Do teachers have a way to contact the front office quickly in the event of an emergency? Yes [ ] No [ ]

In what manner?
Intercom system in every room [ ]
Phone in every room [ ]
School-issued cell phone [ ]
Two-way radios [ ]
Other: _____

(12) Can teachers lock classroom doors from the inside?

Yes [ ] No [ ]

Do classrooms allow teachers and students to hide out of sight from an intruder in the hallway or outside of the building?
Yes [ ] No [ ]
If not, what do you think your classroom needs to make this possible? _____

_____

(13) As a teacher, do you ever feel unsafe in your classroom, the halls, or restrooms during the school day?

Constantly 1 2 3 4 5 Almost never

How often and in what way? _____

_____

Have you been trained how to deal with a threatening student?
Yes [ ] No [ ]
Have you been trained what to do if two students are fighting?
Yes [ ] No [ ]
Have you been trained how to respond if you see a stranger in the halls who obviously should not be there and who might be a threat to students or staff? Yes [ ] No [ ]

(14) Are students in your school required to wear ID badges?
Yes [ ] No [ ]
If so, how well is this working?

[ ] Extremely well – everyone wears their ID badges
[ ] The majority of students wear ID badges
[ ] About half the students wear their badges
[ ] Only a small portion of the students wear their badges
[ ] Practically no one wears the ID badges

What could be done differently to make this effort more effective?

_____

_____

(15) Do you believe that weapons are ever brought into your school?

Constantly 1 2 3 4 5 Never

What weapons are most common, what types of students usually bring them, and for what reasons? _____

_____

(16) Which scenario most closely matches your school's use of metal detectors?

Daily, on all students, as they enter the building [ ]
Fairly often, on all students, as they enter [ ]
Occasionally, on a random basis [ ]
On rare occasions [ ]
Never [ ]

If you feel your school's use of metal detectors is ineffective, how could it be improved? _____

_____

(17) How often are illegal drugs brought onto your campus?

Constantly 1 2 3 4 5 Never

If your answer was other than "5", what types of drugs are most common? _____

_____

What percent of students at your school do you suspect are using illegal drugs at school on a regular basis?

< 1% [ ] 5 – 10% [ ] 21 – 30% [ ]
2 – 4% [ ] 11 – 20% [ ] > 30% [ ]

(18) Do you believe that students bring alcohol onto your campus?

Constantly 1 2 3 4 5 Never

What percent of your students do you feel may be using alcohol at school on a regular basis?

< 1%	[ ]	11 – 20%	[ ]	31 – 50%	[ ]
2 – 4%	[ ]	21 – 30%	[ ]	> 50%	[ ]
5 – 10%	[ ]				

(19) Does your school use dogs for drug searches?
Yes [ ] No [ ]
If yes, with what frequency? _____

Do you feel the dog/handler team that serves your school is effective? Yes [ ] No [ ]
If not, why not and what should be done differently? _____
_____
_____

(20) Do specific groups of students in your school cause the majority of problems on campus?
Yes [ ] No [ ]
If so, describe these groups: _____
_____
_____
How could these groups be better handled? _____
_____

(21) Are your students allowed to leave campus for lunch?
[ ] Yes, all of them
[ ] Yes, but only grade level(s) _____
[ ] Yes, but only students who meet specific criteria
[ ] No students are allowed to leave campus, but many do
[ ] Students never leave campus at lunchtime

Do you believe this is the best arrangement for your school?
Yes [ ] No [ ]
If you answered *No*, what would be more appropriate? _____
_____
_____

(24) Are there any video cameras installed at your school?
Yes [ ] No [ ]
Do you think these cameras have helped security at all?
Yes [ ] No [ ]
If you answered *No*, what would make them more helpful?
_____
_____

(25) If your school has SROs (School Resource Officers) or security staff, do you feel they are effective at handling security related problems?

Not Effective 1 2 3 4 5 Very Effective

What changes would you make as to how these personnel are used, hired, trained etc.? _____
_____
_____

(26) Are students frequently loitering in the halls during class time? Yes [ ] No [ ]
Does anybody effectively stop this? Yes [ ] No [ ]
If so, who? _____
If this is a constant problem, what could be done to improve this situation? _____
_____
_____

(27) Are teachers given monitoring duties in addition to teaching? *(Check all that apply)*
[ ] before and/or after school
[ ] during lunch
[ ] other _____

What do you recommend if you feel these assignments/duties are ineffective at maintaining security? _____

_____

_____

(28) Having completed this questionnaire, which of your security concerns would you rate as the most important to the safety of your school, its occupants, and the community?

Most important: _____
Second most important: _____
Third most important: _____
Fourth most important: _____

Are there any other security-related concerns you would like to mention?_____

_____

_____

_____

_____

_____

_____

_____

Thank you for taking the time to give us your opinion on these issues.

Questionnaire for SCHOOL ADMINISTRATORS and SECURITY PERSONNEL

School Name _____

Date: _____

[Continue longer answers on a separate sheet of paper]

(1) How often has your school been broken into over the past two years? *[Please give the approximate date of each break-in.]*

_____

_____

_____

What type of property was stolen and what was the approximate value? _____

_____

_____

List the vandalism or damage dollar value of that has occurred during nighttime break-ins. *[Describe damage and where it occurred.]* _____

_____

_____

Were the perpetrators of any of these crimes ever caught?

Yes [ ] No [ ]

If so, who were they, in relationship to the school, and how were they initially identified?

_____

_____

_____

(2) Does your school have an intrusion detection (alarm) system?

Yes [ ] No [ ]

To your knowledge, are the sensors walk-tested at least twice a year to make certain that all sensors are operating properly?

Yes [ ] No [ ]

Do you think your intrusion detection system works properly?

Yes [ ] No [ ]

How often (per year) has the system alarmed when there was no obvious break-in? That is, what is the nuisance alarm rate?

_____

_____

Was the cause of these alarms ever determined (i.e., blowing mobiles in classrooms, fallen posters, a staff member returning to retrieve something, etc.)? _____

_____

_____

What are the specific weaknesses of your intrusion detection system (that is, do you think more sensors are needed, sensitivity needs adjustment, sensors are easily defeated, etc.)?

_____

_____

_____

(3) List everyone who is notified when the system alarms, and who actually responds when there is an alarm. _____

_____

_____

How quickly do they generally respond? _____

_____

Has this response group/individual ever come upon a suspect during a break-in and, if so, was the suspect apprehended?

_____

_____

_____

If the expected response to school alarms is inadequate, what do you think could be done to improve it? _____

_____

_____

_____

(4) Are there particular windows, doors, skylights, etc. within your school that you feel are easily compromised by an intruder? Please list these, their location, and any repairs or improvements needed.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

(5) If you arrive at or leave school when it is dark outside, do you feel safe walking to and from your car? Yes [ ] No [ ]

If your response is "No", please explain any concerns you have:

_____

_____

(6) If you believe the nighttime exterior lighting is inadequate, what improvements are needed? _____

_____

_____

(7) Are staff vehicles are safe in the parking lot?
Yes [ ] No [ ]
If not, what do you think should be done to make them safer?

_____

_____

(8) Do you feel that the parent drop-off/pick-up and bus drop-off/pick-up areas are safe from a traffic perspective?
Yes [ ] No [ ]
From a malevolent outsider or insider perspective?
Yes [ ] No [ ]
Are there enough adults assigned to monitor this area?
Yes [ ] No [ ]
If you answered *No* to either question, what improvements do you recommend (for example, installing speed bumps or bollards)?

_____

_____

(9) Do teachers or monitors have two-way radios when on bus duty or assigned to oversee a particular part of the campus?
Yes [ ] No [ ]
Do the radios work properly and transmit adequately from various parts of the campus to the front office?
Yes [ ] No [ ]
If response to either question is *No*, please explain:

_____

_____

(10) Do you think the exterior and grounds of your school campus are well cared for? Yes [ ] No [ ]
How would you rate the exterior appearance of your school on a scale of 1 to 5? (The age of the school should not necessarily be a factor – clean grounds, lack of weeds, pleasant and well-cared for landscaping, maintenance of buildings, etc. are more important.)

Dirty, poor upkeep 1 2 3 4 5 Very pleasant and inviting

If you rated your school less than a "4", specify what you feel the problems are: _____

_____

_____

(11) Do you feel that the interior of your school is well-cared for?
Yes [ ] No [ ]

How would you rate the interior appearance of your school on a scale of 1 to 5?

Dirty, poor maintenance 1 2 3 4 5 Very clean and cared for

If you rated your school less than a "4", specify what you feel the problems are:_____

_____

_____

_____

(12) Are cleaning staff in your school at night? Yes [ ] No [ ]
If so, are they are safe? Yes [ ] No [ ]
If they are not safe, what would keep them safer? _____

_____

(13) How difficult is it for visitors to your school to bypass the office and go directly to a classroom or other student area?

Easy, no one watches 1 2 3 4 5 Difficult, visitors always stopped

If you answered less than a "4" above, what do you think would help this situation? _____

_____

_____

(14) How often are unauthorized non-student persons in your hallways?

Constantly 1 2 3 4 5 Almost never

If you answered other than "5" above, how do you think they enter the school building? _____

_____

_____

(15) How many exterior doors (other than the front office) are left unlocked during the school day in your main buildings?
Most or all [ ] Just a few [ ] Only main entry doors [ ]

How often are exterior building doors left propped open during the day by students or teachers?
Frequently [ ] Occasionally [ ] Almost never [ ]

Do you feel that either of the above needs improvement to keep unauthorized visitors out of your buildings? If so, please explain:

_____

_____

(16) Are teachers always allowed access to their classroom after hours? Yes [ ] No [ ]
If so, how do they get in?
Have key assigned to them [ ]
Custodial crew lets them in [ ]
They call security to let them in [ ]
Other _____

Do all teachers have an access code to turn on/off the intrusion detection system during off-hours?
Yes [ ] No [ ]

Do you feel that teachers and other staff are safe in the building late in the evening if they are by themselves?
Yes [ ] No [ ]

Would it be reasonable to collect all exterior door keys and prohibit staff from entering after hours without previous arrangements? Yes [ ] No [ ]

(17) Do you feel that all staff are adequately trained in emergency procedures at your school for incidents (such as a hostage situation, violent intruder, gas leak, etc.)? Yes [ ] No [ ]

Is the school's emergency response plan reasonable? If not, what is wrong with it? _____

_____

What would make the plan better? _____

_____

_____

(18) Do all teachers have a way to contact the front office quickly in the event of an emergency? Yes [ ] No [ ]

In what manner? Intercom system in every room [ ]
Phone in every room [ ]
School-issued cell phone [ ]
Two-way radios [ ]
Other: _____

(19) Can teachers lock their classroom doors from inside the classroom? Yes [ ] No [ ]

If you are worried about a violent intruder during school hours, do classrooms allow teachers and students to hide out of sight from an intruder in the hallway or outside of the building? Yes [ ] No [ ]

If not, what do you think each classroom needs to make this possible? _____

_____

(20) Do you ever feel unsafe in a classroom, the halls, or in a restroom during the school day?

Constantly 1 2 3 4 5 Almost never

If so, where, and in what way? _____

_____

_____

(21) Have you been trained how to deal with a threatening student or parent? Yes [ ] No [ ]

Have you been trained what to do if two students are fighting? Yes [ ] No [ ]

Have you been trained how to respond if you see a stranger in the halls who obviously should not be there and who might be a threat to students or staff? Yes [ ] No [ ]

(22) Do you give your local police department, fire department, and other emergency response teams an up-to-date layout/map of your campus every year? Yes [ ] No [ ]

Does your school administration and security personnel meet at least once or twice a year with local emergency response teams to discuss security issues and get a walk-through of the campus? Yes [ ] No [ ]

(23) Do students ever falsely pull the fire-alarms? Yes [ ] No [ ]

If this occurs more than once or twice a year, what measures has your school put into place to handle these? _____

_____

_____

(24) Does someone meet buses returning from school events late at night? Yes [ ] No [ ]

Are students and staff encouraged to park their vehicles in a particularly well-lit part of campus when returning to school late at night? Yes [ ] No [ ]

(25) Do all bus drivers have two-way radios or cell phones for use in the event of an emergency? Yes [ ] No [ ]

Do the buses have cameras installed on them to record mischief or malevolent activities? Yes [ ] No [ ]

(26) Does your front office have a covert panic button or duress alarm for security incidents requiring an immediate response? Yes [ ] No [ ]

(27) Are students and staff required to wear ID badges? Yes [ ] No [ ]

If yes, how well has this been working?

[ ] extremely well – everyone wears their ID badges
[ ] the majority of students wear ID badges
[ ] about half the students wear their badges
[ ] only a small portion of the students wear their badges
[ ] practically no one wears the ID badges

What could be done differently to make this effort more effective?

_____

_____

How do you handle students who have forgotten their badges?

_____

_____

_____

Do you badge visitors and, if so, what do you use? _____

_____

_____

(28) Is the campus enclosed with appropriate and effective fencing? Yes [ ] No [ ]

If not, what do you believe is needed, and where? _____

_____

_____

_____

_____

(29) Do you believe that unauthorized weapons are ever brought into your school building?

Quite often 1 2 3 4 5 Never

What weapons are most common, what types of students usually bring them, and for what reasons? _____

_____

_____

_____

_____

_____

(30) Which scenario most closely matches your school's use of metal detectors?

Daily, on all students, as they enter the building	[ ]
Fairly often, on all students, as they enter	[ ]
Occasionally, on a random basis	[ ]
On rare occasions	[ ]
Never	[ ]

If you feel your school's use of metal detectors is ineffective, how could it be improved?

_____

_____

_____

_____

(31) How often are illegal drugs brought onto your campus?

Constantly 1 2 3 4 5 Never

If your answer was other than "5" above, what type of drugs are most common? _____

_____

What percent of your students do you feel may be using illegal drugs on a regular basis?

< 1%	[ ]	5 – 10%	[ ]	21 – 30%	[ ]
2 – 4%	[ ]	11 – 20%	[ ]	> 30%	[ ]

Does your school use any type of drug-detection kit that the school nurse can administer to students believed to be under the influence of drugs? Yes [ ] No [ ]

If not, how does your school generally handle this situation?

_____

_____

_____

(32) Do you believe that students bring alcohol onto your campus?

Constantly 1 2 3 4 5 Never

What percent of your students do you feel may be using alcohol on a regular basis?

< 1% [ ] 11 – 20% [ ] 31 – 50% [ ]
2 – 4% [ ] 21 – 30% [ ] > 50% [ ]
5 – 10% [ ]

(33) Does your school use canines for drug searches?

Yes [ ] No [ ]

If so. with what frequencv?

_____ times per month, or _____ times per year

Do you feel the dog/handler team that serves your school is effective? Yes [ ] No [ ]

If not, why not and what could be done differently? _____

_____

_____

(34) Do specific groups of students in your school cause the majority of security-related problems on campus?

Yes [ ] No [ ]

If so, describe these groups: _____

_____

How could these groups be better handled? _____

_____

_____

_____

(35) Are your students allowed to leave campus for lunch?

[ ] Yes, all of them
[ ] Yes, but only grade level(s) _____
[ ] Yes, but only students who meet certain criteria
[ ] No students are allowed to leave campus, but many do
[ ] Students never leave campus at lunchtime

Have you had troubles either on or off the campus due to this arrangement? Yes [ ] No [ ]

Do you believe this is the best arrangement for your school?

Yes [ ] No [ ]

If not, what would be more appropriate? _____

_____

_____

(36) Does your school enforce a standard attire policy?

Yes [ ] No [ ]

If your school's population is over about 1200 or so, how does the security staff distinguish between students and non-students who don't belong on the campus? _____

_____

_____

(39) Do you feel that your school's disciplinary measures are effective – that students want to avoid them, and therefore cease activities that result in such measures?

Yes [ ] No [ ]

If not, what disciplinary measures would be more effective (and more undesirable to students)? _____

_____

_____

_____

(40) Does your district have an alternative school where students with more serious disciplinary requirements can be assigned?

Yes [ ] No [ ]

How effective do you think this alternative school is?

Not as effective as it should be 1 2 3 4 5 Very effective

What would make the alternative school more effective?

_____
_____
_____

(41) Are there any video cameras installed at your school?
Yes [ ] No [ ]

How many? _____

Are they helpful to your security staff?
Yes [ ] No [ ]

If not, what would make them more helpful?

_____
_____

Are recordings from the video system of sufficient resolution and frame-rate to determine:

What occurred in incidents of concern? Yes [ ] No [ ]
The identity of individuals in the scene? Yes [ ] No [ ]

Are additional cameras needed at other locations on campus?
Yes [ ] No [ ]

If so, where?

_____
_____
_____
_____

(42) If your school has SROs (School Resource Officers) or security guards/aids, do you feel they are effective?

Not helpful 1 2 3 4 5 Extremely helpful

What changes (such as how they are hired, trained, how they respond, the number of SROs, etc.) would improve their effectiveness?

_____
_____
_____
_____

(43) Are students frequently loitering in the halls during class time? Yes [ ] No [ ]
Does anybody effectively stop this? Yes [ ] No [ ]
If yes, who? _____
If not, why not? _____
_____

If this is a constant problem, what could be done to improve this situation? _____
_____
_____

(44) Are teachers given other duties other than teaching? *(check all that apply)*

[ ] before and/or after school
[ ] during lunch
[ ] other _____
[ ] none

What do you recommend if you feel these assignments/duties are ineffective at maintaining security? _____
_____
_____
_____

(45) Having completed this questionnaire, which of your security concerns would you rate as the most important to the safety of your school, its occupants, and the community?

Most important: _____
Second most important: _____
Third most important: _____
Fourth most important: _____

Are there any other security-related concerns you would like to mention?

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Thank you for taking the time to give us your opinion on these issues.

Appendix B: A more technical discussion of formats, resolution, pixels, lenses, and field-of-view

A basic familiarity with camera terminology presented in Chapter 3 is adequate for most school administrators who plan to go out on bid for a CCTV system. However, those who might be responsible for choosing or upgrading camera equipment may need more information. Appendix B presents additional technical information on format, resolution, pixels, lenses, and field-of-view.

Format

Camera format relates to the size of the camera imaging device. Most solid-state cameras used in security applications today are 1/2-inch, 1/3-inch, or 1/4-inch format. There are a few older 2/3-inch cameras still in use. The trend has been to make camera formats smaller as picture element densities have increased. This reduces manufacturing costs per device and allows the production of smaller cameras. One advantage of a 1/2-inch format camera is that there are usually more lens options available.

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 TV lines of resolution. Horizontal TV lines-of-resolution relates to the number of independently resolvable elements (small details) of the picture width. Different types of video cameras can range from 250 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 (including camera, cabling, recorder, and TV monitor) that a school might typically use and that uses a standard NTSC (National Television Systems Committee) color video signal format, 300 to 470 lines of horizontal resolution are common. Black-and-white systems for security applications typically range from 300 to 570 lines of resolution. Cameras with more than 800 lines of resolution are commonly used in broadcast TV, medical, or industrial applications.

Pixels

Pixels, or active picture elements, are directly related to horizontal TV lines of resolution. Active picture elements are the actual number of light-sensitive elements that are within the camera imaging device. They 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 TV lines of resolution relate to picture elements by a three-fourths factor (by definition of horizontal TV lines of resolution) so a black-and-white camera with 768 active picture elements will have 576 horizontal TV 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 sensitivity. Before selecting a camera and lens combination for an application, one must determine what is 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 of criteria. For identification purposes, a person must be much larger in a scene than for the purpose of just determining if a human is present.

Because a camera scene is observed on the TV monitor, the entire video 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 example, a 570-line camera that displays on a 250-line monitor is pointless; too much money was spent on the camera or not enough on the monitor.

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 6 horizontal TV lines across a 1-foot-wide object 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 the accurate identification of a person by facial features, 16 horizontal TV lines (21 pixels) of resolution subtending a 1-foot-wide object is recommended. (This type of resolution has been used successfully for recordings submitted as evidence in a court of law, but this would depend on the situation and the particular court.)

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 appears within the scene, as well as how many active picture elements the object covers on the camera imaging device. Higher-resolution cameras (for example, 570 horizontal TV lines or higher) can be used to distinguish objects farther away (smaller in the scene) than a lower resolution camera (such as 250 horizontal TV lines) allows. In other words, an object can be smaller in the scene for higher resolution cameras and still meet the minimum horizontal resolution criteria. One significant point of this is that fewer higher resolution cameras than lower-resolution cameras may be needed in some interior and many exterior applications. Also, for long views such as in, say, exterior parking lots, a higher-resolution camera may be cost effective, where in an interior scene, the width of the field-of-view may

never get very wide, i.e., for a long hallway, a lower-resolution camera may be just as good.

Lenses

A camera lens focuses light reflected from objects within a scene onto the imaging device of the camera (see Figure 8.1). 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 (discussion is further in this chapter) 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. Mismatched camera and lens formats can be used satisfactorily in a few instances, but the installer must be aware of the view desired.

Except for the more uncommon sizes, there usually is not a significant price difference between various lens sizes. The most common sizes are 4.8mm, 5.6mm, 8mm, 12mm, 16mm, 25mm, 50mm, and 75mm. A 75mm 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 usually involved.

The important thing to remember is that the field-of-view in feet depends on the focal length and format size. The field-of-view is expressed in horizontal and vertical angular (in degrees) fields-of-view. Most manufacturers or vendors who sell lenses with their cameras can provide charts that list the angular fields of view for common lens sizes. Figure 8.2 shows the difference between two different lens focal lengths.

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. In other words, a 16mm focal length lens will have a clear aperture of 8mm. The lower the F-number of a lens, the more light 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 1.2 to 1.8. 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

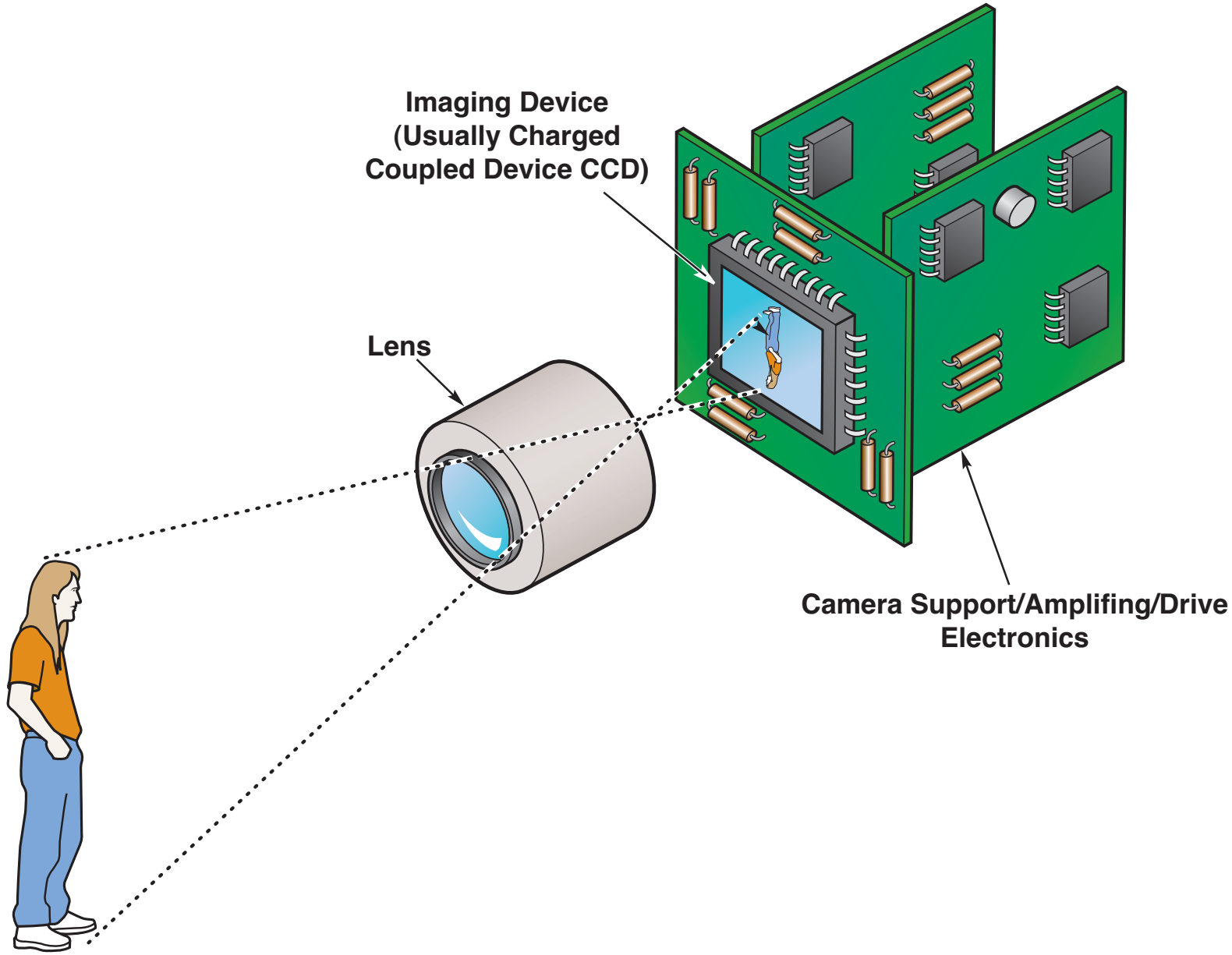


Figure 8.1 Basic CCTV camera components.

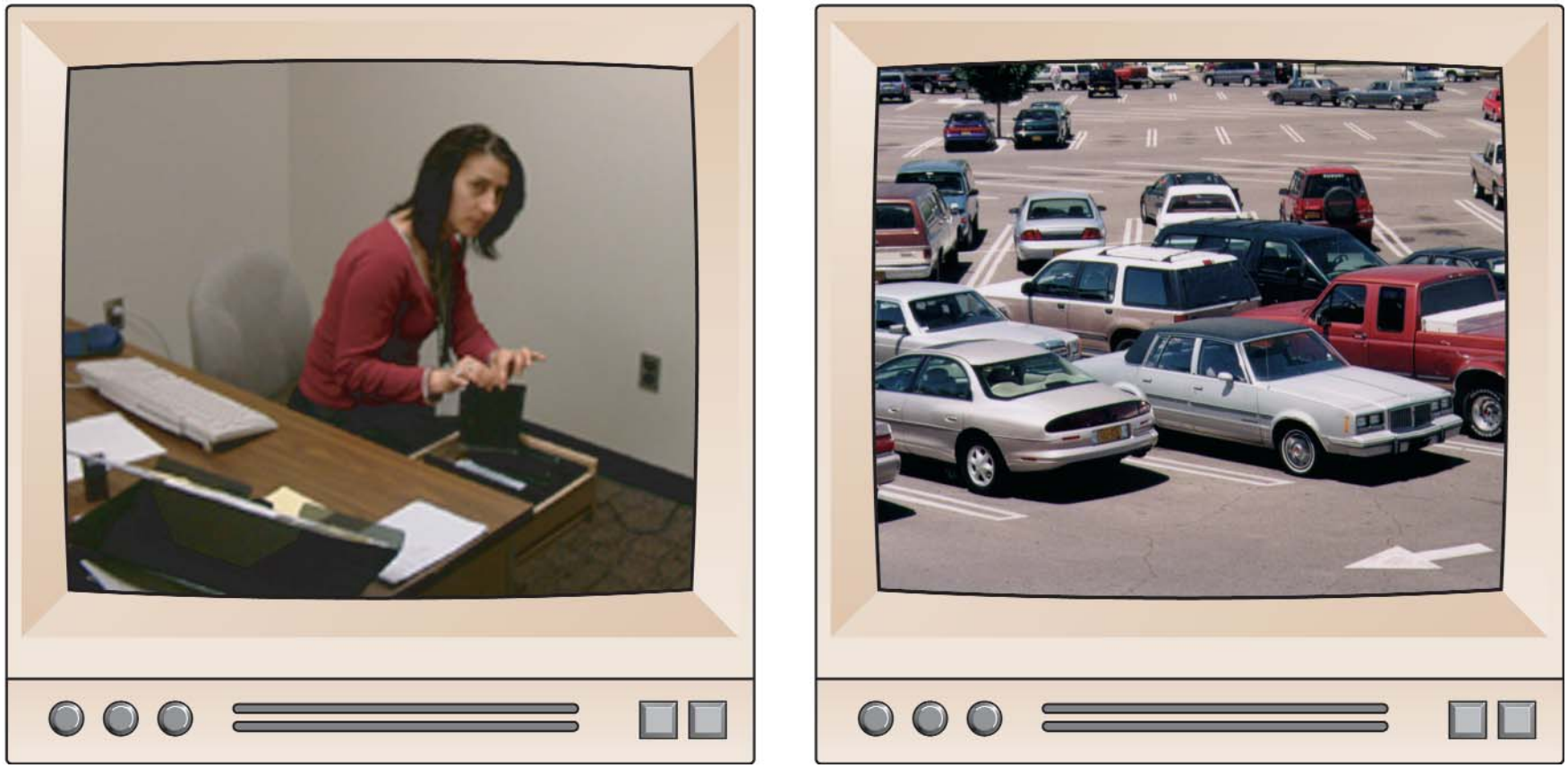


Figure 8.2 The left-hand image demonstrates a camera lens focal length of 4.8mm. The right-hand image uses a focal length of 16mm.

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) 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 some interior applications, an auto-iris lens will be necessary.

A 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 receives. Electronic shutters have limitations, however. They may not have as much range as auto-iris lenses. This is an important consideration for exterior applications. Some manufacturers use both an auto iris and an electronic shutter within their cameras in order to provide the widest range of successful applications.

Field-of-view

Field-of-view (FOV) relates to the size of the area that a camera will see at a specific distance from the camera. The field-of-view is dependent on lens focal length and camera format size.

The FOV width and height can be calculated using the following formulas:

FOV Width (feet) = (Width of imager (horizontal in mm) x Distance from camera (feet)) divided by Focal length (mm)

FOV Height (feet) = 0.75 x FOV width

Manipulating the FOV formula allows a calculation of the distance in feet from the camera for a required FOV width. The formula becomes:

Distance (in feet from camera) = (FOV width (feet) x Focal length (mm)) divided by Width of imager (horizontal in mm)

Before the FOV for a camera is selected, the minimum desired resolution for an intruder or object to be viewed must be determined (i.e.,

whether it is desired to identify a person or to just determine that a person is within the scene). This will limit the maximum FOV width and is referred to as the resolution-limited FOV (see Figure 8.3). The resolution-limited FOV width can be determined by using camera resolution in horizontal TV lines per foot and the number of lines of resolution per foot required to identify an intruder. The following formula is used to calculate the resolution-limited FOV width:

Resolution-limited FOV width = Camera resolution divided by Number of lines of resolution that is acceptable to identify an intruder

A resolution of 16 lines per foot is considered acceptable for identifying most people. If a camera with 350 horizontal TV lines of resolution is utilized, the resolution-limited FOV width for a resolution of 16 lines per foot can be calculated as follows:

Resolution-limited FOV width = 350 divided by 16 = 22 feet

The following table presents the camera imager format sizes and their associated image width. Example: Calculate the maximum distance from a 350-line, horizontal resolution, 1/2-inch format camera with a 75mm lens to the resolution-limited FOV width at 16 lines per foot resolution.

Distance = (22 x 75) divided by 6.4 = 258 feet

Figure 3 illustrates that there is camera coverage beyond the resolution-limited area but the resolution will decrease as the distance from the camera increases. People may be seen but not identified beyond the resolution-limited FOV. The Figure also demonstrates that, as people walk toward the camera and into the blind area, they disappear from view starting with their feet.

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.

Another method of calculating the field-of-view is to use an electronic lens calculator, available on camera and lens manufacturer's websites. (For example, see www.cohu.com.) A less expensive but effective option is the circular slide-rule-like field-of-view calculator, available free from some camera manufacturers. See Figure 8.4.

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.

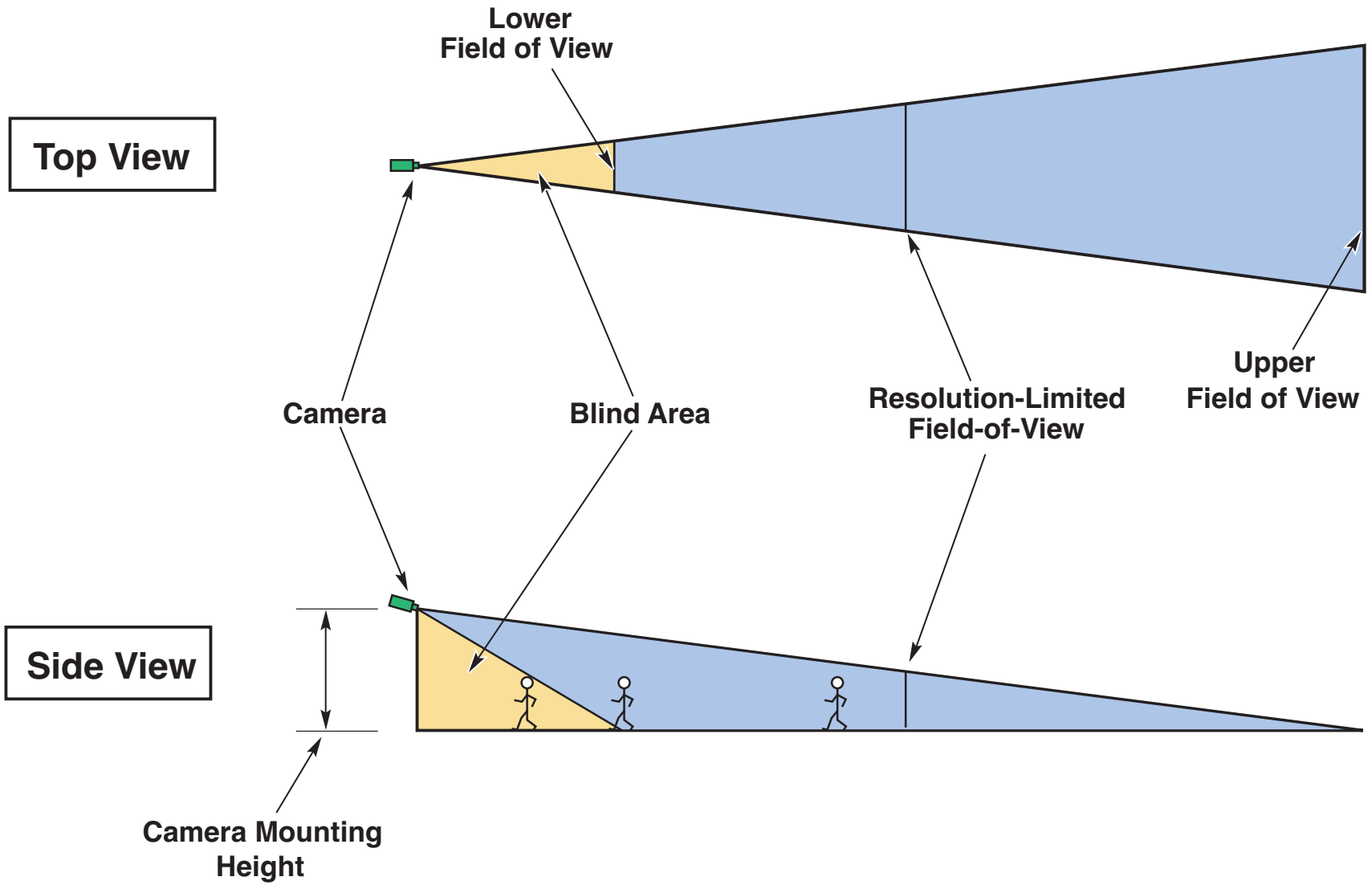


Figure 8.3 This diagram depicts the field-of-view for camera coverage.

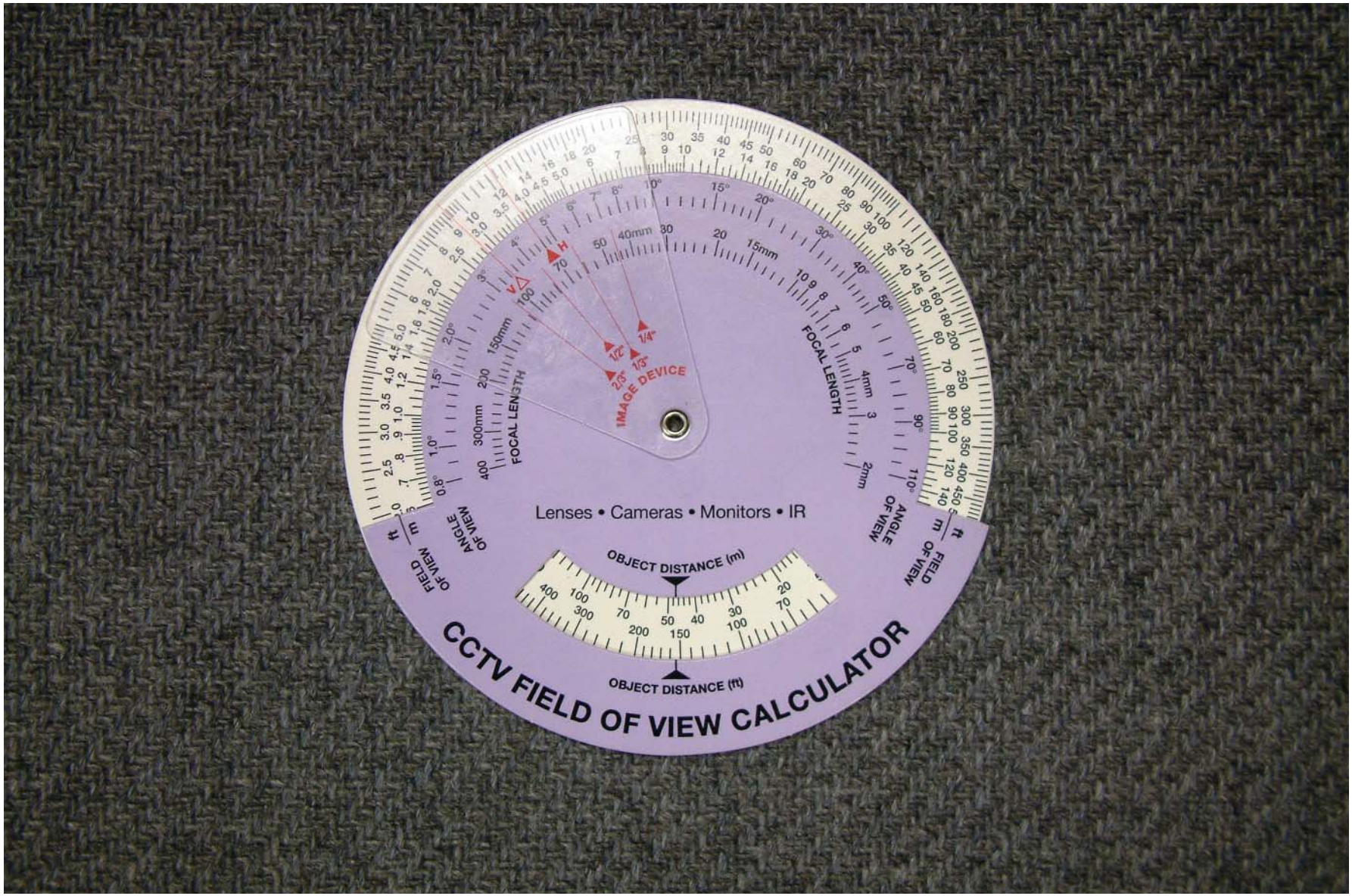


Figure 8.4 This photo shows one example of a field-of-view calculator that was free from a camera manufacturer.

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, wide screen monitors, recorders, and signal transmission equipment must be considered also. Cameras are specified with the number of horizontal TV lines of resolution and active picture elements. Black-and-white security cameras typically have a horizontal resolution between 500 and 600 lines, while color cameras for security applications typically have 300 to 470 lines.

Appendix C: Resources on security and safety in schools

This appendix provides several recommended resources (government and non-profit) on security and safety for individuals seeking further information. The lists presented below in alphabetic order are not exhaustive, but are representative of the many resources available to administrators.

Organizations with information on school security and safety

American Association of School Administrators (AASA)
1801 North Moore Street
Arlington, VA 22209
Phone: 703/528-0700
www.aasa.org

This is one of education's longstanding professional organizations. AASA often teams with other organizations on projects focusing on safer schools. One of the categories covered in the Issues and Insights section of their website is Safe Schools. Included there are numerous links to articles, reports, related websites, and resource centers. The AASA conferences link contains information on its annual conference and exposition, association-sponsored learning seminars, web casts and conferences, and summer institutes.

American Society for Industrial Security (ASIS)
1625 Prince St.
Alexandria, VA 22314-2818
Phone: 703/519-6200
www.asisonline.org

A primary focus of this organization is to increase the effectiveness and productivity of security professionals, by developing educational programs and materials focusing on the fundamental as well as the latest advancements in security management. ASIS sponsors a variety of courses and seminars, an annual seminar and exhibit, publications, a trade journal and a security industry buyer's guide. Educational Institutions is an ASIS Standing Committee. The ASIS website has a great deal of information with useful search options.

Center for Health and Health Care in Schools (CHHCS)
1350 Connecticut Ave., Suite 505
Washington, DC 20036
(202) 466-3396
www.healthinschools.org/sh/emerg.asp

CHHCS is a nonpartisan policy and program resource center located at The George Washington University School of Public Health and Health Services. It is designed to be a one-stop shop that provides school leaders with information they need to plan for any emergency, including natural disasters, violent incidents and terrorist acts.

Center for the Prevention of School Violence (CPSV)
1801 Mail Service Center

Raleigh, NC 27699-1801
Phone: 800/299-6054 or 919/733-3388 ext 332
www.cpsv.org

Established in 1993 at the North Carolina State University as one of the nation's first school safety centers, the Center serves as a primary point of contact for dealing with school violence. Its resources and services include presentations, materials, workshops, program development, maintenance, research, and evaluation.

International Association of Campus Law Enforcement Administrators (IACLEA)
342 N. Main Street
Hartford, CT 06117-2507
Phone: 860/586-7517
www.iaclea.org

The mission of IACLEA is to advance public safety for educational institutions by providing educational resources, advocacy, and professional development. Its membership includes campus law-enforcement directors and staff, criminal-justice faculty members, municipal chiefs of police, companies offering campus law-enforcement products and services, and colleges and universities throughout the U.S., Canada and the UK. Information on IACLEA's annual summer conference and other events is listed on its website's Calendar of Events.

International Association of Professional Security Consultants (IAPSC)
525 SW 5th Street, Suite A
Des Moines, IA 50309-4501
Phone: 515/282-8192
www.iapsc.org

A non-profit professional association of independent, non-product affiliated professional security consultants. The IAPSC Web site includes a directory of security consultants, speaker's bureau listing, and available media services and upcoming events.

National Alliance for Safe Schools (NASS)
Ice Mountain
P.O. Box 290
Slanesville, WV 25444-0290
Phone: 888/510-6500; or 304/496-8100
www.safeschools.org

A non-profit corporation, NASS was founded in 1977 by a group of school security directors to provide technical assistance, training, and publications to school districts interested in reducing school-based crime & violence. NASS products & services include school security assessments, educational programs for troubled youth, training programs (for administrators, teachers, and students), various publications, and safe school workshops.

National Association of School Resource Officers (NASRO)
1601 Northeast 100th Street
St. Anthony, FL 32617
Phone: 888/316-2776; or 941/232-4633
www.nasro.org

A non-profit organization made up of school based law enforcement officers and School Administrators, NASRO serves as the largest training organization for school based law enforcement and school administrators in the nation. NASRO sponsors an annual training conference each summer and conducts regional seminars and tailored training in the area of school safety preparation

National Association of School Safety and Law Enforcement Officers (NASSLEO)
P.O. Box 3147
Oswego, NY 13126
Phone: 315/529-4858
www.nassleo.org

An organization for persons who are interested in the law, practice and politics of school-related safety considerations, NASSLEO provides leadership in security planning & training and in maintaining information about the role of school security in today's educational community. NASSLEO sponsors an annual conference each summer

National Crime Prevention Council (NCPC)
1000 Connecticut Ave. NW 13th Floor
Washington, D.C. 20036
Phone: 202/466-6272
www.ncpc.org

The mission of NCPC is to enable people to create safer and more caring communities by addressing the causes of crime and violence and reducing the opportunities for crime to occur. NCPC services include publications, training, facilitation and technical assistance, public service advertising, and conferences.

A major thrust of the Council is its Youth Safety Corps with a mission to recruit, train, and mobilize a student population to improve the learning environment of America's schools by designing and running projects to prevent youth crime, violence, and drug abuse. The NCPC website maintains a calendar of regional and national conferences which focus on crime prevention, public safety and security.

National Criminal Justice Reference Service (NCJRS)
P.O. Box 6000
Rockville, MD 20849-6000
Phone: 800/851-3420, or 301/519-5500
www.ncjrs.org

NCJRS is a federally funded resource offering justice and substance abuse information to support research, policy, and program development worldwide. Its sponsors include all bureaus of the U.S. Department of Justice and the Office of Justice Programs (which includes the Office of Juvenile Justice and Delinquency Prevention). NCJRS is an extensive source of information on criminal and juvenile justice in the world.

Services available through the NCJRS website include:

NCJRS Abstracts Database which provides summaries of 180,000+ criminal justice government

reports, journal articles, and books, all of which is searchable on the web; NCJRS Virtual Library that provides for searching of 7,000+ full-text publications; and an events calendar of conferences, workshops, seminars, and other events relating to juvenile and criminal justice and drug control policy.

National Resource Center for Safe Schools – The Safetyzone
Northwest Regional Educational Laboratory
101 SW Main St. Suite 500
Portland, OR 97204
Phone: 503/275-9500
www.safetyzone.org

This center was established through a cooperative agreement with the U.S. Office of Juvenile Justice and Delinquency Prevention and collaborates with state and local agencies, professional organizations, technical assistance providers and others. Its services include assistance in developing safe school plans, training and technical assistance, information dissemination, and collaboration to refine a variety of materials on school safety. The Safetyzone website provides links to a variety of publications and to a calendar of school safety events.

National School Boards Association (NSBA)
1680 Duke Street
Alexandria, VA 22314
Phone: 703/838-6722
www.nsba.org

NSBA is a nationwide advocacy outreach organization for public school governance whose library serves as a central information resource for all members and staff. An area of particular interest is the legal aspect of public school policy and procedure. Links on the NSBA website include Publications & Reports and Conferences & Training. In addition to its annual conference, the Conferences & Training link includes information on many regional workshops and seminars and to a number of online training courses.

National School Safety Center (NSSC)
141 Deusenberg Drive - Suite 11
Westlake Village, CA 91362
Phone: 805/373-9977
www.nssc1.org

This is an independent information center and clearinghouse sponsored by the U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention with emphasis on technical assistance, referrals, consultant services, library services, conferences, meetings and a speakers' bureau in the areas of school vandalism, prevention, delinquency, school safety, drug education, drug abuse, and dropout prevention.

U.S. Department of Education
400 Maryland Ave. SW
Washington, DC 20202
Phone: 800/872-5327
www.ed.gov and www.ed.gov/emergencyplan

The Department's website contains a wealth of useful information including guides, publications, resource directories, grant information, rules & regulations, full-text publications, and a search tool with links to various education related programs and websites. The Department pledges to keep its website current and pertinent to educators, parents and students. An Events link through the department's Press Room has access to a list of upcoming events and calendars of activities and happenings. The emergency planning guide published by the Department of Education can be found at their website: www.ed.gov/emergencyplan. Two Department entities that have specific references for school security are:

Office of Safe and Drug-Free Schools (OSDFS)
U.S. Department of Education
400 Maryland Ave. SW
Washington, D.C. 20202
Phone: 202/401-5842

Education Resources Information Center (ERIC)
ERIC Project c/o Computer Sciences Corp.
4483-A Forbes Blvd.
Lanham, MD 20706
Phone: 800/538-3742
www.eric.ed.gov

The Education Resources Information Center (ERIC) is a vast digital library of education-related resources. Its mission is to provide a comprehensive, easy-to-use, searchable, Internet-based bibliographic and full-text database of education research and information. The database now includes more than 1.1 million citations and covers the topics of school security, safety, and violence, along with legal issues and the use of technology in these areas. The U.S. Department of Education website contains a link for locating and ordering department publications via ERIC.

Other websites related to school security

There are literally hundreds of websites with valuable information and resources on the topics of School Security, School Safety, School Violence and Prevention, etc. Only a few of the more relevant sites containing information on School Security have been listed here.

National Clearinghouse for Educational Facilities (NCEF)
www.edfacilities.org

With a mission to serve as a resource for the nation's school personnel and allied professionals who plan, design, construct & maintain educational facilities, the NCEF acquires, manages, and disseminates information relating to educational facilities. NCEF's new web page, Safe School Facilities, addresses those aspects of school buildings and grounds that help ensure the physical security of school occupants during a variety of natural and man-made threats. The NCEF Calendar provides information on educational facilities-related events taking place nationwide.

National School Safety and Security Services
http://www.schoolsecurity.org/resources/crisis.html

Safe Schools Coalition, Inc.
www.thesafeschools.org/

A nonprofit organization of volunteers dedicated to helping colleges and schools to be safe and healthy whose major function and purpose is to foster the exchange of information among organizations, their members and others. Accordingly the organization's website contains links to many related organizations in addition to links to grant information and event information.

National Youth Violence Prevention
Resource Center
www.safeyouth.org

A website containing resources for professionals, parents and youth working to prevent violence committed by and against young people. These resources include information on conferences, funding, materials, organizations, technical assistance, media, publications, and other applicable topics.

U.S. Department of Justice Office of Community Oriented Policing Services (COPS)

1100 Vermont Ave. NW
Washington, D.C. 20530
Phone: 800/421-6770; or 202/307-1480
www.cops.usdoj.gov

The mission of the COPS Office is to advance community policing in jurisdictions of all sizes across the country. Over the past several years, COPS has supported several collaborative partnerships between law enforcement agencies and local schools. Among the topics covered on the COPS website are available print and online resources, training, and funding opportunities.

Security Industry Association (SIA)
635 Slaters Lane Suite 110
Alexandria, VA 22314
www.siaonline.org

SIA is an international trade association which provides education, research and technical standards to promote growth, expansion and professionalism within the security industry. Its web site has links to training opportunities, standards, and industry meetings and events. SIA is the sole sponsor of the ISC (International Security Conference & Exposition) Conference and Expo which bi-annually presents the most recent advances in the security industry.

Conferences and meetings on school security

Many of the professional organizations listed above sponsor an annual conference or seminar for members. Some organizations have provisions for non-member participation in all or part of these events. Contact the sponsoring organization for dates and locations of these conferences.

Many of the government and non-profit organizations listed above maintain a calendar of school security and safety related workshops, conferences, training sessions, etc. on their website.

These organizations include:

National Criminal Justice Reference Service (NCJRS)
www:ncjrs.org

U.S. Department of Education
www.ed.gov

National Alliance for Safe Schools (NASS)
www.safeschools.org

National Crime Prevention Council (NCPC)
www.ncpc.org

National School Boards Association (NSBA)
www.nsba.org

American Association of School Administrators (AASA)
www.aasa.org

National Association of School Resource Officers (NASRO)
www.nasro.org/

International Association of Campus Law Enforcement Administrators (IACLEA)
www.iaclea.org

National Resource Center for Safe Schools – The Safetyzone
www.safetyzone.org

National Clearinghouse for Educational Facilities (NCEF)
www.edfacilities.org

Safe Schools Coalition, Inc.
www.thesafeschools.org/

Other major security industry seminars and conferences include:

American Society of Industrial Security (ASIS)
Annual Seminar & Exhibits
www.asisonline.org

Asisonline.org holds an annual seminar and exhibit that includes educational sessions, certification sessions, ASIS Security Marketplace bookstore, and more than 800 exhibiting companies with numerous product demonstrations. The event is usually held in September and the location varies.

International Security Conference & Exposition (ISC)
Sponsored by: Security Industry Association (SIA)
www.siaonline.org

This bi-annual conference includes seminars and workshops that are organized into core conference tracks which reflect major security topics, and more than 500 exhibitors which showcase security equipment. The seminars and workshops generally include sessions specific to school security. The ISC East conference is usually held in New York in the fall; the ISC West conference is usually held in Las Vegas in the spring.