School Security Technologies

National Clearinghouse for Educational Facilities

Tod Schneider
April 2009

Due to rapid changes in security technology, this publication is updated quarterly. It replaces Newer Technologies for School Security*, published by the ERIC Clearinghouse on Educational Management in 2001, and* The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies*, published by the U.S. Department of Justice in 1999.*

See the related NCEF publications Mass Notification for Higher Education *and* Selecting Security Technology Providers*.*

Look before You Leap

Over the past decade electronic security technology has evolved from an exotic possibility into an essential safety consideration. Technological improvements are coming onto the market almost daily, and keeping up with the latest innovation is a full time job. At a minimum, a basic understanding of these devices has become a prerequisite for well-informed school security planning.

Before resorting to high-tech security solutions, school officials should think carefully about the potential for unintended consequences. Technological fixes may be mismatched to the problems being addressed. They can be expensive.. Any network will require continual maintenance, eventual upgrading, and constantly updated virus protection and Intrusion Detection Systems (IDS) to watch for hackers or unauthorized transfers of data. A full-blown information technology (IT) department will usually be essential.

An over-reliance on electronic technology can also backfire with power outages or technological failures. Some security technologies raise political and philosophical concerns. That said, technological solutions can also be highly functional and cost effective. The pros and cons must be weighed carefully within the context of local sensibilities.

Don't start by choosing a technology and looking for a problem it can solve. The process should be the reverse: Identify and prioritize the problems before jumping to solutions, and analyze solutions carefully before committing funding. It's not uncommon for districts to invest in a particular technology district-wide before analyzing and prioritizing the real concerns of the individual schools. Every school should be capable of quick lockdowns and evacuations, but the details beyond that can vary considerably. Some schools are in rough neighborhoods where violence is endemic, others are not. Some schools are constrained by meager budgets, others have deep pockets. Leaky roofs may take precedence over electronic access control systems.

Partial measures can prove to be wasted investments. Secure front doors are of little value if back entries remain uncontrolled. Metal detectors and ID cards won't stop bullying behavior, nor will security cameras stop offenders all by themselves, as has become all too evident at many school shootings. On the other hand, comprehensive access control and improved emergency communication systems are usually good investments.

Access Control

If windows and doors are left unsecured and unsupervised, the choice of access control device is of no consequence. But once a school has committed to controlling access, decisions have to be made about which technology to use.

Door Locks and Latches

Most doors lock with a spring latch, dead latch or deadbolt extending from the door into a strike plate on the door jamb. Spring latches are fine for holding a door shut against the wind, but are relatively easy to defeat by prying, or in some cases by sliding a credit card through the gap between door and jam. Dead latches offer more security, but the bolts are still relatively short and tapered. Deadbolts are the most effective, squared off rather than tapered, and extending about an inch beyond the edge of the door when thrown. However, fire code dictates where specific types of deadbolts can or cannot be used. Designated exit doors cannot be deadbolt-locked when areas are occupied. Any of these devices can be controlled manually or electronically. See the NCEF publication, *Door Locking Options in Schools*.

Lock-and-Key Systems

In many cases, conventional lock-and-key systems are still the best option. Indicators that they are not would include the following:

- Burglaries in which thieves accessed locked rooms and there were no signs of forced entry.

- Lost keys or a history of distributing keys that were not stamped "Do not duplicate." The stamping should discourage duplication, although it is no guarantee that it will not occur.

- Lockdown plans which are heavily dependent on the extensive use of keys. If the keys are carried by only some staff members, or if the act of locking the doors would put teachers in the line of fire, or if teachers are likely to be physiologically stressed during the crisis, then an alternative plan is worth considering.

Electronic Access Control Systems

If any of the above are concerns, consider door hardware that automatically locks, classroom doors that can be pulled shut to lock without inserting a key, electronic entry-control devices such as programmed wireless fobs or proximity cards, or hard-wired control switches for instantaneous lockdowns. Some campuses are considering remote lockdown abilities from central consoles at strategic locations on- or off-site.

Electronic controls can be integrated into almost any type of door, including hinged and sliding models, turnstiles, or revolving doors. If opting for this approach, it's usually far more economical to build in the devices during initial construction.

There are a few basic down-sides to electronic controls: initial costs, programming difficulties and power outages.

Costs. If installation is integrated into initial construction it's likely to be more affordable than if installed as a retrofit, but in either case is considerably more than the cost of conventional lock hardware. Wireless technology may reduce installation costs. In any case, the cost may prove worthwhile in the long run. Electronic key cards can be cancelled instantly with a few key strokes, telling the system to reject the card if it is presented, and can even send an alert to tell a supervisor that someone has attempted to gain entry using the cancelled card—a far more efficient option than changing all the locks, or pleading with a fired employee to return a key.

Technical difficulties. Someone has to install and run the software, updating information whenever a new card is issued or old card is cancelled. At the front end, this includes creating cards for all users. Someone has to replace lost cards and issue new ones. If the people who know how to operate or repair the equipment are unavailable the system can be derailed, at least temporarily.

Power. All systems should have emergency back-up power. The alternative is complete systems failure during any power outage.

Early models of keyless entries involved push-button coded locks, which were often compromised through unauthorized access to codes. An early electronic model was the swipe card, which involved passing a card through a slot—a device that proved vulnerable to vandalism. Nowadays most models involve simply holding a coded fob or card within close proximity to the reader (hence the term "prox" cards). Vehicles can have readers installed on their dashboards, to automatically open gates.

Location. Electronic controls are not needed at every door, but can be used selectively (especially ito keep costs down.) If a facility's outer doors are secured electronically, internal areas might be adequately secured with conventional locks. Electronic locks may be worth considering for doors to higher security areas as well, or for areas that a school would prefer not to have to supervise. For example, if the parking on the west side of the building is for staff only, the west side door can be unsupervised, allowing entry only to those who carry access cards. Cards can be issued to temporary workers or contractors, programmed to open only certain doors during specified days and hours. Schools have no need to worry about losing keys, since the cards are cancelled when the job is completed. Cards can serve multiple functions, acting as debit, library, or identification cards as well.

Whether devices are free-standing or tied into a central processor, if they are too accessible they may be vulnerable to technologically savvy intruders. As a precaution, it may be wise to install lock activation devices or relays on the secured side of the installation, in line with the conventional security panel approach.

Biometrics. Fingerprint scanners, iris readers, hand vein readers, and facial recognition technology are options to consider for high-security locations, but their use in public schools is still rare, controversial, and not especially practical. There is considerable concern about the implications of entering such data into databases that could find their way into government files or the public domain. At the least, parental consent forms should be considered, and privacy provisions tightly worded. Which biometric feature is used as an identifier — iris, fingerprint, etc. — is not overly significant at this point. Decisions should be based on functionality, cost, and maintenance considerations.

In some cases, doors may be normally left unlocked during working hours, but should be easily secured during a lockdown. A lockdown button at the reception desk is invaluable for this purpose, empowering the receptionist to instantly secure the school against an approaching threat.

Piggy-backing/tail-gating. A glaring weakness in access control is the ease with which intruders can slip in close behind legitimate users. Often this is with a gesture of courtesy from the first student, who holds the door for someone behind him, or when the first student is too intimidated to confront the person who "piggybacks" on their entry. If this is commonplace at your school, access control measures may be illusory, providing a false, and counterproductive, sense of security, although they may at least reinforce territoriality. To address this problem, the issue is not primarily what type of access device is used, but what response measures are in place. Options might include: (1) video analytics or on-site security personnel that trigger alarms when piggy-backing occurs, (2) video recording of the incident to identify the intruder, and (3) an access control response, such as a lockdown of a second door preventing further entry coupled with an immediate response from security guards to confront the intruder. Training for all legitimate users goes hand-in-hand with these tighter measures. Some high-tech turnstiles and revolving doors now on the market incorporate proximity cards, infra-red beams, and analytics, which can detect and photograph tailgaters or unauthorized intruders, denying them access or identifying them for follow-up, at costs ranging from $50,00 to $75,000 per revolving door or $13,000-45,000 per turnstile.

Visitor Badging

In most public schools, visitors don't receive access control cards, but they do receive visitors' badges in order to make them easily spotted while on campus, and more to the point, to make people who are not wearing badges more noticeable. Schools use widely varied levels of screening before issuing badges. In some cases visitors can walk in and pick up stickers without having to clear any kind of screening – a self-serve operation that has minimal value, but is fairly commonplace. In other cases visitors are obliged to introduce themselves and present ID. More extensive systems may check fingerprints, sex offender registries or school-maintained data bases. Other features include time-deactivated badges, which fade out or change color after an allotted amount of time. More comprehensive products can scan I.D., take digital photographs, print bar-coded badges and issue parking permits. Rarely is there an effective process in place to retrieve visitors' badges after visits, or to oblige visitors to check out. Because of the wide variety of options, schools should carefully consider what they want to accomplish with visitor badging before investing in a product.

Surveillance Equipment

On top of cost, maintenance, and effectiveness issues, surveillance cameras raise some serious philosophical concerns. The mere presence of cameras can suggest that the environment is dangerous, reinforcing fear and undermining the school climate. Americans are particularly wary of empowering an Orwellian government to watch over citizens, and surveillance cameras are classic icons of such an arrangement. The issue is worthy of some attention. On a pragmatic level, appropriately used cameras are merely affordable substitutes for placing staff members in the halls to watch over our children, with better memories and an endless attention span. What could be wrong with that? The distinction is that in functional schools, human monitors are more likely to engage in pro-social interactions with students, offering a smile, a pat on the back or a kind word. Cameras don't offer positive reinforcement; their role is perceived as strictly negative, catching students doing something wrong and preserving evidence against them. From this perspective, cameras may be seen as more akin to grim prison guards than to nurturing teachers. Moreover, depending on how accessible or permanent the recordings become, youthful indiscretions or victimizations conceivably could haunt or humiliate

children indefinitely into the future. For all of these reasons, it is essential that clear policies be developed about the use of cameras, access to the images and length of preservation. Students and their families—not just school officials--should have equal access to recordings that can exonerate them from accusations.

What conditions justify installation of surveillance equipment? Surveillance technologies are appropriate when (1) offenders need to be identified, and their actions documented; (2) hidden areas are attracting problem behaviors that have not been successfully deterred through other measures; (3) the location filmed is semi-public and there should be no reasonable expectation of privacy; (4) risks are higher than average, such as in an overseas embassy school that may be targeted for political reasons, or in a residential treatment program where there may be a heightened risk of abuse or false accusations; and (5) when vandalism, bullying, or other problems persist despite other interventions.

Technical issues. Surveillance camera systems have proved most useful in identifying suspects after the fact. In most cases, employees cannot constantly watch electronic monitors to catch misbehavior at the moment it occurs—they have other job duties, and staring at a live broadcast of the hallway all day would constitute cruel and unusual punishment. But live viewing can be used selectively, and can deter some criminal activity, at least when students realize their behavior is being taped. “Smart” cameras can help alert supervisors in some cases as well (see ***Video analytics***, below). Cameras should be mounted well out of reach and should be secured in opaque domes or similar enclosures that protect against vandalism while obscuring the camera’s coverage area. Outdoor cameras may need heated or cooled housings for extreme weather. Cameras in corrosive, dirty or extremely humid environments can also require protective housings. Wily criminals can still avoid the cameras, or wear disguises to obscure identities. For this reason, install cameras in overlapping patterns, so that every camera is within the recorded view of another. It may also be useful to have some covert cameras capturing images around the corner from the main event, where offenders may not have thought to disguise themselves.

If components are going to fail, they are most likely to do so fairly quickly. Have spare components on hand for replacement purposes.

Problem locations, such as specific bus routes or classrooms, can be brought back under control by installing cameras and advertising their presence. Cameras targeting dark areas usually require infrared (IR) capabilities.

Camera Options

Hard-wired alternatives. The distance between a camera and a receiver will affect the quality of images received, even with hard-wired systems. Standard coaxial cabling will suffice for distances of up to 1,000 feet; fiber-optic cabling can go further. Repeaters can boost the range considerably. Industrial strength routers make it possible to install wireless cameras almost anywhere. Power-over-Ethernet (PoE) capability has made it possible to install cameras anywhere intranet cabling already runs, saving the substantial cost of running power cabling. (There are some limitations on distance with PoE, usually about 300 feet, although this can be doubled with a mid-span expander.) PoE can power most electronic technologies, including alarm keypads, access readers, fire alarms, and cameras, Cables should be encased in metal conduit or otherwise protected from vandalism or accidental damage. Any installation that leaves cables exposed to vandals is inadequate. For isolated locations, solar-powered cameras are now on the market as well. Wireless mesh networks, routers, and repeaters are discussed further on p.9.

High-definition (HD) versus analog. High-definition cameras are the state of the art option. Analog cameras represent the older technology, usually at a much more attractive price, but likely to become obsolete in the years to come. The main difference between the two is that HD “forensic quality” digital images can be enlarged without losing definition—up to a twelve fold increase over traditional analog recordings, and this will only continue to grow as technology improves. Even a good analog camera image resolution of 640x480 can be inadequate if the picture needs to be enlarged to more than double the size. An HD camera can produce a 1280 x 1040 megapixel image that can be enlarged much more dramatically without losing definition.

One application can be seen with cameras designed exclusively to capture license plates in low light conditions, a feature that cost $30,000 just a few years ago but costs closer to $300 to $3000 today. Lighting, distance, reflections, and movement each place different demands on license plate cameras, driving up costs.

Capturing a license plate on a car stopped at a gate is simpler than capturing a plate on a fast moving vehicle.

Because of band width, processing power limitations, and lighting needs, 1.3 megapixel HD cameras are a good size to aim for today. Any higher capacity may overwhelm the recording and band width capacities of your equipment. Within a year or two, larger capacity HD cameras will make sense, when the recording devices catch up to them. Some medical facilities are already using 10 megapixel HD cameras, and a network video recorder system recently came on the market that can handle 16 megapixel images, 160 times the density of an analog image. The greater capacity found with megapixel cameras means that in addition to being able to enlarge pictures without losing definition, it's possible to cover broad areas efficiently and effectively. A few new cameras can replace five or ten old ones and deliver crisper images.

Fixed versus moving (pan-tilt-zoom, or PTZ) cameras. Fixed cameras tend to require much less maintenance and can be relied upon to catch targeted locations. Moving cameras cover more areas, but require more maintenance and can miss critical details of an incident. One option is to integrate cameras into duress-alarm systems; cameras remain fixed unless alarms are triggered, at which point cameras pan to the alarm locations. PTZ cameras also can be monitored and redirected with a joystick by a security officer. Zoom lenses require higher lighting levels.

Lens options. Lenses are generally fixed or varifocal. Fixed lenses are fine if you know ahead of time the precise distance of the area you want captured; varifocal lenses can be adjusted on site, providing an option for wider fields of view as needed, This flexibility makes installation easier and has been the industry standard for many years. Megapixel lenses will be needed for megapixel cameras with an equal capacity; that is, a 5 megapixel camera should have a 5 megapixel lens to get best use of both components. Megapixel lenses can capture far superior images that can be enlarged considerably. For capturing an area wider than 70 degrees, a rectilinear megapixel lens corrects fisheye distortion;360-degree lenses can be used for comprehensive coverage of large areas to help detect intruders, manage crowds, or enhance overall situational awareness.

Color versus black and white. Color cameras are usually most effective under well lit conditions, while black and white cameras are more effective at night. Infra-red lights can improve night time recording.

***Calibration and Tuning*.** Calibration and adjustments for changing seasons, along with lighting conditions, can require regular adjustment with older cameras—meaning more maintenance is required. Some newer "smart" cameras on the market (such as the VideoIQ iCVR) will make these adjustments automatically.

Video analytics: specialized, "smart," or "intelligent video" cameras versus conventional equipment. Conventional cameras impassively collect images. Smart cameras use algorithms to spot selected shapes or movements — such as people entering through an exit, leaving a suspicious package, lingering in a suspicious location or a short-term parking space, hopping a fence, or falling down, as well as tampering with, blocking or attacking the camera — and send immediate alerts. They can sort images based on time, date, alarm notification, object, size, location and color, count the number of people who move through a door, determine attendance at large events, help analyze pedestrian traffic patterns, and read license plates. This technology is still relatively young, but improving rapidly. In the future they may be able to analyze "unusual behavior" in an environment.

Centralized versus distributed systems. With centralized systems, all the data collected by a camera is usually sent to a "head-end" for processing. With analog cameras, this is often a DVR; with a networked video system the "head-end" is usually a PC server. But processing power and on-board memory capacity on internet protocol (IP) cameras is improving, making it possible to beef up algorithms and retain data on the cameras themselves, taking some of the load off of centralized servers. Transmission of high-resolution images only occurs on an as-needed basis, such as when an alarm is triggered. This distributed approach, using "edge" installations, minimizes band-width usage, and maximizes scalability, cost-effectiveness, and flexibility in general.

Capacity issues. There are two critical issues to consider when selecting equipment: storage capacity (how many gigabites of memory) and active processing (CPU) capability. It's possible to gather a huge amount of information, but if you try to juggle it all at once the computer may become overloaded. If you've ever experienced a slow computer, you know what this is about — their ability to multi-task is severely limited. This becomes significant when you are drawn to a variety of

Intelligent Video options, and want to use them all. For example, video analytics can be used to trigger an alarm when someone crosses a fence. Other software might try to capture faces, and watch for them elsewhere in the facility. Still other software grabs license plate numbers. The swipe of a card at an entry point could tap into a data base and pull up a picture of a student requesting entry at a guard station. All of these options have a certain allure, but that doesn't mean your computer can apply all of them at once—which is why a professional systems integrator should be guiding the process of selecting hardware and software. Specifications for new software should be analyzed to determine compatibility with available hardware's processing power. Quad-core processors are quickly becoming essential minimums. High resolution MPEG cameras may be more than some analytic software can handle at present.

Real versus fake cameras. Occasionally, schools consider using fake cameras as cheaper deterrents. While that might have some benefit, there are two downsides to this approach. No surveillance occurs, and people may be misled into thinking they are in an area being supervised when in fact they are not.

VCRs versus DVRs versus NVRs. The camera is only one piece of the surveillance system in which quality can vary considerably. Another critical piece is the recording device—and recording devices are having a hard time keeping up with camera improvements. Ancient systems recorded analog images onto reels of film that had to be developed before viewing. Those archaic systems were surpassed by video cassette recorders (VCRs), using tapes that deteriorate and are cumbersome to search. The next evolution was to digital video recorders (DVRs). DVRs work well unless you anticipate upgrading the quality or number of cameras, at which point the DVR may reach capacity and require replacement. For that reason, especially at the institutional level, DVRs are now being gradually overtaken by network video recorders (NVRs). NVRs are generally installed on the edge of a local area network (LAN) as part of an internet protocol digital video surveillance system (IPDVS). As memory-needs grow, the server memory can be upgraded without having to overhaul the system. (See **Integration and Convergence**, below.) Good NVRs and DVRs should be highly reliable, capable of self-diagnosis and self-repair, and able to send alerts to designated staff when alarms are triggered. Images that can be pulled up on the internet, either in recorded or live mode, can be useful for emergency responders or school administrators (for example, Chicago police and 911 centers are currently upgrading their system to monitor 4500 school cameras and send images to patrol cars during emergencies.) A number of devices are now available that promise to bridge the gap between older and newer technology, such as by converting analog information into digital information in a customized DVR. In some cases these may provide a means of keeping down costs by deferring the replacement of older cameras, but only if they work as advertised. Schools that already have run coaxial cable for VCRs might find it economical to use it for DVRs. If that cabling is not in place, and if an ethernet is already in place, the NVR may be more economical.

The next major change on the horizon is a jump from NVRs to Cloud computing, in which the "head-end" functions are outsourced to massive off-site computing centers (see discussion on p.14.)

The larger the memory capacity of cameras and systems, the greater the detail, number of frames per second, and days of recording are possible before available memory is filled. Be specific about the minimum quality of pictures and number of days of recording you require. A year ago, a 16-camera analog system with a 240-Gigabyte DVR sounded reasonable. A school system today should be looking into high definition cameras — around 1.3 megapixels — and should set aside at least 1-3 terabytes of storage on their network server. When purchasing components, it is essential to actually see not just the live image broadcast, but the recorded image accessible after the fact, and the printed result, field-tested on-site before finalizing a purchase. Focal length, equipment limitations, and the weather can all impact the quality of images generated, but lighting is a critical factor. The higher the number of megapixels, the more lighting will be needed. Test any equipment being considered under low-light as well as changing conditions (day and night, rainy and clear).

Bus-mounted systems. Misbehavior has led many districts to install surveillance cameras covering the interior of buses as well as entry areas, with both video and sound capabilities. Systems are available that allow remote viewing and wireless downloading.

Weapons Detectors

Another form of electronic surveillance is the metal detector, a device which raises some concerns. Detector portals, at $3,000 to $8,000 apiece, are expensive in their own right, but staffing them can be a budget-buster, involving three to eight security officers at each entry for an hour or two every morning. Portals are of questionable value unless all other passages for weapons delivery, such as windows or back doors, have been sealed, and unless the students have absolutely no contact with the outside world until they leave for home. Portals aren't effective with backpacks or other items that contain numerous metal objects, and as a result an X-ray scanner will also be needed, starting at about $30,000. Rather than reassuring students, metal detectors can be fear-reinforcing.

Funneling students through detector portals poses serious logistical problems:

- Students waiting to gain entry are likely to form a crowd outside the school, where they are easy targets for violence.

- Boys and girls grouped together have a tendency to posture for each other, which can induce "showing off" behaviors that can include violence. This can lead to the need for gender-segregated entries at separate portals.

- Scheduling may become untenable, as students cannot make it through screening in time for class. This can require students to show up much earlier for school, or to stagger class times. (In large sites, express lanes can offer faster passage to students who know they won't trigger alarms; if they do they'll be sent back to the other line.)

Unfortunately, the overall message conveyed, as with cameras, can be that the school is trying to catch wrong-doing instead of rewarding positive behavior. Very few schools use detectors, and that makes sense; most have never had a shooting and never will. Some do have enough behavioral warning signs, however, that detectors need to be considered.

Hand wands may be a better investment than portals for two reasons: affordability (they cost hundreds of dollars, rather than the tens of thousands of dollars it costs for portals and x-ray machines), and portability (they can be used in any location at a moment's notice). Some schools have found sweeps of randomly chosen classrooms with hand wands to be a more practical approach. Scanning all students who are late or lingering in halls is another option which, if nothing else, motivates students to get to class on time. Battery life is short, so have back-up wands or batteries handy.

Communications

Everybody on campus should be able to call for help, pass along a timely warning, or receive a warning, at any time, anywhere. A teacher shouldn't have to choose between staying with students and calling for help. Weaknesses in communication systems often include:

- Unreachable areas, such as playgrounds, bathrooms, boiler rooms or basements, due to lack of radio reception, wiring, speakers or phones.

- Dysfunctional equipment that works inconsistently, due to bad weather, leaky roofs or deferred maintenance.

- Reliance on towers or systems that predictably overload in genuine emergencies.

Communications Equipment

Radios and related issues. Radios should be high priorities for daily operations as well as for use during emergencies. While inexpensive, off-the-shelf radios may be tempting, they are inadequate for school use; they won't offer the many needed options, and they don't operate on the frequencies reserved by the FCC for school districts. Anyone can use them, and as a result they will quickly overload in emergencies. They're designed in most cases for simplex use, meaning one person talks, the other listens, and that's all. More sophisticated systems with dozens or hundreds of users will want a "trunked" repeater or similar radio system, which can function like cell phones, and can also permit messages to be broadcast to multiple users simultaneously. Professional quality radios can cost $400 to $5,000 each, not including monthly fees for repeater use and maintenance. A Kenwood TK-3173 analog handheld unit might run $400 to 500, while a digital upgrade could run $1300 for a Kenwood TK-5310, or $2,000 to $3,000 for a Motorola XTS 5000 series.

Resist OPM (other people's money) syndrome. Bear in mind that grant money runs out. Eventually more radios will be needed. When that time comes, high end models may no longer be affordable.

Analog versus digital. Generally speaking, digital radios have clearer sound at a much higher price. Analog radios have more static at a much lower price. At range limits analog radios can experience excessive static, but digital radios shut down entirely. Recently, firefighters have run into problems with digital "vocoder." technology designed to enhance speech but sometimes drowns it out by enhancing nearby emergency equipment noises and alarms. Manufacturers are working to fix this problem. Contrary to rumor, the FCC is not requiring a shift to digital radios, or to a "P25" format. The P25 format is only meaningful for multiple government entities crossing into each others' jurisdictions and being able to talk to each other. The FCC mandate is to switch to narrow band by 2013, effectively squeezing more bands into a limited number of channels. Most analog and digital radios can be programmed to do this. Eventually radios may very well move entirely from analog to digital technology, but the costs are not yet competitive and in most cases, primarily based on costs, analog radios still make more sense. At the same time, blindly accepting the lowest bids is a very risky approach that can saddle the school with substandard equipment or services.

Batteries. Radios should be kept in battery chargers every night. Extra batteries should also be kept charged up for use in prolonged emergencies; otherwise radios can be rendered inoperable at the end of one 8-hour shift. Compare the types of batteries compatible with the radios to find what serves you best. Nickel metal hydride make good sense for schools based on how long they'll last on a charge and how often you can recharge them. Lithium ion batteries are significantly lighter, but less forgiving; if they're allowed to run completely out of power they can't be recharged. NiCad batteries are a reasonable third option falling between these two.

Purchasing a system. First invite local vendors to assess your specific needs. Do you need cell phone or GPS (global positioning system) tracking capabilities, or just basic radio contact? How many radios and channels will be needed? Are you located in an urban or rural area? Have them explain how they can meet your needs. Do they have their own towers and repeaters already in place, or would they have to install them? Who maintains the equipment? Who handles FCC requirements and licenses? If your towers go down, do the handheld units retain direct-talk capability within individual schools? If towers are already in place, drive throughout the area and test vendors' radios extensively to identify any dead spots. Make sure their prices reflect discounts negotiated through coalitions, such as the Western States Contracting Alliance. Finally, ask for references, and check on them.

Dead spots. Even with multiple towers, additional measures may be needed to extend radio range into highly insulated locations, such as basements or tunnels. In those cases, consider running coaxial cabling (such as Radiax) from an omni-directional antenna, through a repeater on the outside of the building, into the secluded area. Another, much smaller, omni-directional antenna will then have to be installed inside the building. Antennae are designed to serve designated frequencies, such as 450-470 Mhz, used for handheld radios in a school setting. IPolice and fire radios operate on another, exclusive, frequency that would require an entirely different antenna, cabling and repeater array, and a similar arrangement would be needed for cell phones, which are discussed shortly. In some cases, frequencies may be too close together, causing interference, in which case filtering arrangements would be necessary. One of these arrays would be needed for each building, at a cost of $4,000 and up.

Channels. Professional radios should be programmable, with enough channels to meet your needs. For example, a district of twenty schools would need a bare minimum of two handheld units per school, and additional radios for facilities staff, custodians, transportation, the superintendent's office, all emergency team members and all school resource officers, totaling at least 50 radios with 26 channels just to get started. In most cases, three times that number of radios would be closer to meeting actual need. A good system could have 20 channels, each with up to 250 "codes", or sub-channels, to choose from.

GPS. Buses or other fleet vehicles with separate radios installed exclusively for GPS use can be tracked continually from a base unit.

Other radios. Police and Fire radios will operate on exclusive channels, at different frequencies from school radios. Software allowing interoperability between school and public safety radio systems exists, but is not widely used. In emergencies, one system may work while others fail. Citizens' band and Ham radio groups, working with disaster response groups can be life savers when other technologies collapse.

Telephones. Hard-wired phones in all classrooms and offices, for the moment at least, are still sound

investments. Teachers and students can rely on finding them in the same location whenever needed, and "enhanced" 911 (E911) systems, which are now fairly standard, should automatically tell call-takers where emergency calls are coming from, depending on the configuration of the on-site phone system. Caller ID can be invaluable for identifying sources of inappropriate or menacing calls.

Cell Phones. Wireless phones manufactured within the past three years should have similar capabilities, but performance isn't yet perfect. Currently, when an E911 center receives a 911 call from a cell phone, it should be able to identify the phone number and the closest cell tower. For 95 percent of Americans the system can also pinpoint the location of the phone itself. School districts should check with their local 911 center and cell phone providers to determine actual performance locally, and should update phone software regularly (contact the individual provider for details on over-the-air, or OTA, programming). None of the systems now on the market distinguish between varying altitudes; in other words, they cannot determine if a call is coming from the first or fifth floor of a building.

Portable devices offer great flexibility — teachers can call for help anywhere at any time, as long as they have a charged phone handy and good reception. (Some districts provide cell phone stipends to employees, with the understanding that they will keep the phones handy during work hours. This eliminates concerns about employee abuse of district equipment and extends communication capabilities at reduced cost to the district.)

Cell phones in student hands can be lifesavers, but they can also be disruptive and, in some cases, tools used for cyber bullying. Camera phones allow students to capture student activity and post it on the web in a manner that can be psychologically devastating.

Phone lines and cell phone towers are both susceptible to overload and storm damage, which undermines reliability, just when they may be needed the most. In some cases radios make more sense than cell phones, economically and logistically. They are less likely to get overloaded, and cost less in the long run, once monthly fees are compared. Some devices combine cell and radio capabilities into one unit, at a premium monthly price *(see discussion below on radios).*

The likelihood over the near future is that someone nearby will almost always have a cell phone. At the same time, some school construction is so dense that cell phones cannot function reliably indoors.

Solutions for cell phone dead zones are similar to the options discussed for radios previously, but at much greater expense. In addition to installing cell towers on campus, and/or internal and external antennae, repeaters and coaxial cabling, cell phone systems will require the installation of bi-directional amplifiers, or "BDAs". Unlike the "passive" Radiax cabling discussed under "radios", BDAs are "active" devices which boost transmissions in dead zones. They are necessary because cell phones are a lot less powerful than hand held radios. A radio might be rated at 4 watts; a cell phone by contrast is closer to ½ watt. Transmit either type of message through a hundred feet of cable and the power of transmission is diminished. BDAs can cost tens of thousands of dollars. In a large institution, such as a university, a cell phone service provider might be amenable to funding installations in exchange for exclusivity, but if you wanted numerous cell phone companies' services to function you would need to coordinate all providers and create a "neutral host" using fiber optic cabling and a distributed antenna system (DAS), which could cost considerably more.

In extremely isolated conditions such as in wilderness schools, in locations where cell phones don't work and where hard-wired phones are non-existent, satellite phones are well worth looking into, along with solar recharging devices. The primary drawbacks to satellite phones are the price, the need for a clear view of the sky, and the need for operable satellites in the right location. Satellite phones usually won't work indoors or underground unless attached to an aerial. Reliance on traditional high-orbit satellites often leads to choppy communication and spotty connections, with gaps between transmission and receipt. By linking a group of Low Earth Orbit (LEO) satellites together, a mesh network is formed that makes service more instantaneous, seamless, and robust; if one satellite fails or is overloaded, the others compensate. Large arrays of LEO satellites are now being launched that eventually will extend radio and internet service to the most remote parts of the planet.

Repeaters and routers. Wireless technology has expanded communication options considerably, but without cell towers or repeaters along the way, most wireless devices won't be able to send messages very far, if at all. Sparsely populated areas may not contain enough customers to justify the expense of constructing towers. Installing wireless routers and repeaters

throughout a campus or community, in some cases as joint projects with municipalities or emergency responders, can make going wireless a viable option. If indoor reception is a problem, see the earlier discussions under cell phones and radios. Wireless routers or mesh networks can extend wireless capacity throughout a campus or geographic area. For example, during the 2008 Olympics, 38 square miles of downtown Beijing were served by 1,000 networked wireless cameras. Mesh networks send information between multiple nodes, with built in redundancy, so that if one path fails another can cover for it.

Intercoms. Intercoms can be integrated into school telephone systems or can be free-standing products. They should make it possible to make announcements school-wide as well as more selectively. Intercoms can be augmented with cameras and call-buttons at entries. Visitors can buzz the office and request admittance, a nice feature when concerned about unwelcome visitors or when unable to actively supervise an entry. Wireless technology may offer some cost savings in installing new systems, and existing WAN or LAN systems can provide a framework that new intercoms can tap into.

Public address systems. These can be hardwired and installed in fixed locations or they can be portable. Portable systems may include wireless microphones that clip onto speakers' clothing, or they can use handheld microphones. Systems can be plugged into conventional outlets or can run on rechargeable batteries. Wheeled cases are useful for hauling systems across campus. The town of Blackwood, in South Wales, is installing loudspeakers directly linked to monitored security cameras. Operators will be able to speak directly to people in view, deterring misbehavior or offering assistance.

Call boxes. Emergency call boxes can be installed throughout a campus, to make it easy for students to call for help. They can be made more useful by adding other features, such as speakers that tie in to a public address system.

Megaphones. When all other technology fails, due to downed lines or cell towers, megaphones provide an easy alternative that can be used in directing mass evacuations or broadcasting messages. Bull horns run on conventional batteries that should be checked and replaced or recharged on a scheduled basis. The wattage directly correlates to the distance the device can project sound — 3 watts will travel perhaps 100 yards, while 25 watts can carry 1,000 yards. Determine the distance for which you would need coverage before making a purchase.

Alarms

Fire alarms can be triggered by smoke or flame, or set off by manually operated pull stations. Extremely sensitive devices can be triggered by a lit match, similar to the alarms used in airplane lavatories. These can respond with audible alarms or recorded messages, or by triggering an alert at a monitoring station. Protective covers that must be lifted, or glass covers that must be broken, discourage false alarms by triggering a local noise alarm first, drawing attention to the person pulling the handle. "Intelligent" fire alarm systems, such as one recently installed at New England college, can detect tampering with room detectors, sending an alert to a monitoring station that pinpoints the location of the activity.

Hard-wired panic button alarms can be built into intercom, phone or burglary alarm systems, or can independently trigger buzzers or lights at monitoring stations.

Burglary alarms can be triggered by door or window entry, acoustic or vibration-based glass breakage or passive infra-red (PIR) detection, which detects temperature changes if someone enters the room. These can be augmented with cameras or microphones that record and transmit images and sounds to hard drives, monitoring stations or web sites.

Annunciators. Similar to burglar alarms triggered by door or window entry, these devices make noise at the point of intrusion and alert staff members at a monitoring station that an emergency door has been opened. If surveillance cameras are used, staff can instantly view the activity.

Wireless alarms can be integrated into pendants, key fobs, radios, equipment, or vehicles. First generation devices (such as body alarms) merely make noise; second-generation devices send messages that identify the person assigned to the device and in some cases can pull up useful data, such as the person's photograph, stalking complaints, or medical concerns, but may not be able to pinpoint their immediate location.

Tracking devices. Third generation wireless alarms can identify the location of a person or item carrying a device in real time, using GPS, radio frequencies, or similar technologies. They can be triggered manually, by pushing a panic button, or automatically, by being moved past a reader. For example, if an extended capability radio frequency identifying device (RFID, or transponder) is implanted inside the case, a computer carried out of the media room might trigger an alarm. This would be an active or semi-active system. A passive RFID can only be read if passed quite close to a reader, like bar codes in stores. Tracking devices can be used to monitor the location of any asset, including school buses — a useful option in case of hijacking. The greatest weakness with satellite-based GPS devices is the need for a direct view of the sky in order to function. In urban areas, tracking systems that rely on network-based triangulation, cell towers, wireless networking, and television signals may be more effective.

Emergency Notification Systems (ENS)

For most K12 schools, emergency notification systems are quite rudimentary, using sirens or bells to convey pre-determined on-site messages, such as "evacuate" or "shelter in place," with varying degrees of confusion or success. Taken up a notch, an emergency notification system will include a PA system, intercoms, telephones, or radios. Families and the general public rely on messages faxed to the media and subsequently broadcast on local radio and television stations in order to learn about events. For many districts, that might be as much as they can afford. But in cases where something more is desired, the trend is toward commercial emergency notification systems that send customized messages to myriad devices. One survey released in January 2008 found about 45 percent of school districts in the United States were using a mass notification system. Costs are the most common obstacle mentioned, ranging from $1 to $5 per student per year, through service providers such as ParentLink®, schoolmessenger®, schoolreach®, alertnow®, Honeywell instantalert®, k12alerts®, blackboardconnect®, teleparent®, e2Campus™ and many others. Initially designed purely for emergency notification, these devices rapidly evolved to offer additional features, such as conducting surveys, advising about student absences or school closures, or recruiting volunteers on short notice. One school, for example, used their system to recruit parents to fill sand bags and move furniture when nearby riverbanks were overflowing. Systems can make it easier for teachers to exchange individual notes with parents of students, offering praise or asking questions. Language translation services also may be integrated into the system. In most cases, parents are required to fill out contact information forms at the beginning of the school year. School secretaries then must enter this information into data bases that are passed on to the ENS provider. Then parents often can update their contact information online at any time.

The most advanced systems are more often seen at colleges and universities, and are geared toward reaching students rather than parents. For an in-depth discussion of mass notification systems, see the NCEF publication *Mass Notification for Higher Education,* www.ncef.org/pubs/notification.pdf.

Integration and Convergence

Many school districts around the country have recognized the value of integrating all data entry into one data bank, eliminating costly redundancy and making it infinitely easier to crunch data (see the Schools Interoperability Framework, or SIF, at www.sifinfo.org). In the same vein, most large institutions have found value in tying all security components into a shared system. If your school plans on using multiple types of security technology, such as cameras, alarms, communication, and access control devices, those components' hardware and software must be not only compatible, to maximize their usefulness, but fully integrated. If you have cameras on the front door, for example, they should be tied in with a monitor in the office and a lockdown button. If you use proximity cards at entries, you might want to tie those into a database that pulls up the card holder's photograph and identification information. This kind of interconnectedness is best guided by a professional systems integrator, someone who knows which components are compatible, has a good track record, and will be available for further consultations down the road if things go wrong. Integration, however, is a field that continues to change as well, now evolving into a field known as "convergence."

A year or two ago, merely going digital and tying all the parts together was considered fairly forward thinking. This usually involved linking devices on varied platforms and incompatible software. Engineering such a feat was often ungainly and prone to difficulties. That's not good enough anymore. The new wave is moving all security

technologies to an IP model — everything feeds into the same network. This not only assures compatibility, but builds in significant additional features. Any Ethernet-based device is effectively monitored for failures 24/7. For example, if an alarm system fails, the failure itself sends an alert to a monitoring station. The risk in this kind of convergence is if the network can be compromised by hackers or viruses. For this reason a dedicated virtual network is a safer way to go, protected from equipment failure with redundant network computers.

In Conclusion

Before investing in security technology:

- If considering multiple devices, fully involve your IP manager and a convergence expert from day one.

- Identify and priority-rank the problems you want to address or the risks you want to mitigate, such as hurricanes, intruders, drive-by shootings, graffiti on the north wall, bullying in the cafeteria, or smoking in the bathroom. Each of these requires very different solutions, only some of which involve high technology.

- Beware of mission drift. Always go back to your originally identified problem and ask yourself, "Do the solutions we chose match the problems we wanted to address?"

- If technology is part of your planned solution, emphasize quality and performance more than low bids. Inexpensive cameras and recorders generally produce less useful images. Inexperienced installers are more likely to make mistakes or go out of business.

- Include generators, back-up batteries, or other secondary power sources. Without them your system may fail just when you need it them most.

- Do your homework. Research makes and models of equipment and seek out first-hand reports of their effectiveness. Many schools have moved boldly into the high-tech security arena, for better or for worse. Seek out these pioneers and take advantage of their lessons learned. Nobody is in a better position to counsel schools about what works and what doesn't.
- The more specific your request for proposals the better. Allowing vendors to use an "equivalent" device rather than the one you have identified may result in a lower bid using a substandard device that doesn't hold up. Consider asking for two kinds of bids, some meeting your specifications and others without those constraints. Then compare the two to see if new options should be considered.

- Make full payment contingent upon functionality and be specific about what "functional" means, such as "A recorded image of two similarly dressed individuals at 2 a.m. at the rear gate shall be clear enough to identify and distinguish between them."

- Finally, remember that security technology cannot solve all school security problems. Integrate technological solutions into broader prevention and intervention measures, ranging from practicing crisis response drills to building a positive school climate.

What's New this Quarter

Satellites collide. While satellites can help us circumvent terrestrial communication technology limitations, they also have some vulnerabilities — a catastrophic collision of two satellites 500 miles above earth in February created a hypersonic shock wave that shredded the structures, spreading a huge amount of debris that could jeopardize all other satellites for the next ten thousand years. This was the first time two intact high speed spacecraft have ever collided, but with satellite use growing annually, the likelihood of further collisions grows as well.

Flash drive Trojan horses. Malware-infected USB drives are a cause for growing concern for anything network-based on campus, including security systems. The U.S. Department of Defense had to order employees to stop using all external media because their network was getting infected. It requires devices to be scanned before use. Cornell initiated walk-in "clinics" to clean devices on campus, and found problems with one out of six devices. http://campustechnology.com/articles/2008/12/usb-device-nightmare-becomes-reality.aspx

Personal Locators. Students who want their families to be able to find them 24/7 now have the option of subscribing to the mobile "pocketfinder." This small GPS device can be accessed by internet or phone to show exact locations in real time; http://www.pocketfinder.com

Radio enhancements. Elektrobit Corporation has developed a satellite/terrestrial connectivity module that eventually may allow emergency responders to route communication through satellites when terrestrial networks fail. (Urgent Communications, January 09.) EFJohnson Technologies now produces a GPS-enabled microphone that can be plugged into most radios to keep tabs on personnel scattered throughout locations during a major incident. (Urgent Communications February 09). Cellular Specialties is introducing a 700/800 MHz signal booster this quarter designed to "maintain clear, uninterrupted communications for first responders in basements, stairwells and inner offices." (http://urgentcomm.com/mobile_data/news/cellular-specialties-signal-booster-20090316/

On the Horizon

Satellite advocacy. A coalition of satellite-communications providers has asked Congress to require emergency networks supported in part by federal dollars to use tools that can operate on both terrestrial and satellite networks. Satellite capability can be built into devices for as little as $5 per device. (Urgent Communications March 09).

Partnerships between universities and vendors to develop new security systems and products may provide cost-effective options for some schools looking for ways to afford new systems ("EFJ Partners with Virginia Tech," Urgent Communications, May 18, 2008, http://urgentcomm.com/mobile_data/news/efj-virginia-tech-0514).

Cell phones are changing the school telephone landscape. Most students now reject land-line phones, bringing their own cell phones instead. Rather than leasing land lines to students, universities may consider leasing cell tower space to providers, or providing their own competitive cell phone plans. New Jersey's Montclair State University gave GPS-enabled cell phones to all 16,000 students. They are intended to serve as "portable information kiosks," covering everything from class assignments and cafeteria menus to emergency messages. They can also serve as instant polling devices for teachers and portable panic buttons with timer features ("Have Phone Will Travel," College Planning and Management, April 2007 [not online]).

Cell phone/911 automatic tracking capability is almost fully in place in Public Safety Answering Points (PSAPs) nationwide.While this upgrading continues, the industry is already looking ahead to Next Generation 911 (NG911), which will apply IP technology and "intelligent" software to deliver almost any kind of information that can be found electronically. For example, nearby surveillance cameras could be triggered when a nearby 911 call is placed ("So Close Yet So Far," Urgent Communications, June 1, 2008, http://urgentcomm.com/networks_and_systems/mag/radio_close_yet_far/index.html). Full implementation of NG-911 is now not expected before 2011 or later (Urgent Communications 2009).

Hybrid satellite-terrestrial networks could extend wireless capabilities to presently unserviceable locations. The mobile satellite services industry (MSS) is in the trial stage of developing this technology ("Satellite Gets Back into the Game," May 1, 2008, Urgent Communications, http://urgentcomm.com/mobile_data/mag/radio_satellite_gets_back).

Handheld radio design may see a major improvement in terms of programming over the next few years. The technology is just getting rolling in the military, and eventually will find its way to police departments and other emergency responders. These "cognitive" systems will find, and move talk groups to, available frequencies within an available spectrum. Airwaves could be pooled rather than parceled out. The cost of radios, if produced en masse, could drop dramatically. Eventually, this improvement could trickle down to the schools ("Cognitive Radio Heads for Finish," Urgent Communications, November 1, 2008, http://login.urgentcomm.com/wall.aspx?ERIGHTS_TARGET=http%3A%2F%2Furgentcomm.com%2Fmobile_voice%2Fmag%2Faffordable_cognitive_radio_1101%2Findex.html

Camera quality continues to improve. The recently approved H.264 standard is "80% more efficient than JPEG and 50% more efficient than MPEG-4.". (Securitymagazine.com March 09.) Essentially, this new approach to compression compares frames and only saves frame-to-frame changes, which means it needs a lot less bandwidth or storage space. Cameras using this technology should now be coming onto the market. Equally important, switch and storage capacity are increasing to accommodate newer camera technology ("H.264 Compression Delivers More with Less," Security Magazine, April 1, 2008, http://www.securitymagazine.com/Articles/Column/BNP_GUID_9-5-2006_A_10000000000000298310).

Power over Ethernet (PoE) is expected to double its abilities with a new standard, 802.3at, which should be ratified by the IEEE this quarter. Boosting the standard from 15.4 to 25 watts will allow it to support more powerful devices, such as heated cameras or infrared illuminators, http://www.sdmmag.com/CDA/Articles/Feature_Article/BNP_GUID_9-5-2006_A_10000000000000511488

Chromatic sensitivity is likely to improve in 2009, along with other fine tuning, enhancing intelligent video's capacity to distinguish between or find individuals based on characteristics such as clothing colors and height ("A Post-Camera Society," Security Magazine, August 12, 2008, http://www.securitymagazine.com/Articles/Column/BNP_GUID_9-5-2006_A_10000000000000398771

Cloud computing through an IP SAN (storage area network) may very soon become an attractive option for clustering storage entirely off-site, beyond DVRs or NVRs entirely. With this outsourcing, SAN's may replace "Redundant Arrays of Independents Disks" (RAIDS) and "Direct Attached Storage" (DAS) as well, because of greater capacity, scalability and other factors. Local devices would send and retrieve data from servers over an IP network. A third party might crunch the data as well before sending it back. The advantages would include endless memory capacity (possibly in the "petabytes" – one petabyte is the equivalent of one quadrillion bytes) and the elimination of a lot of on-site hardware and software, and related maintenance costs. Security Magazine, January 2009, "Clusters, Clouds and the Future of Storage."

Fingerprints and biometrics may eventually replace credit card signatures or ATM codes. In one system that has been operational since 2006, the card itself has an imbedded fingerprint reader. If the prints don't match, the card won't work ("Smartmetric Announces That Your Fingerprint Will Make Credit Card Signatures and ATM PIN Numbers a Thing of the Past," Reuters, May 9, 2008, http://www.reuters.com/article/pressRelease/idUS211364+09-May-2008+MW20080509). Other software relatively new to the market uses voice biometrics as the equivalent of a fingerprint (for example, VoiceVerified, www.voiceverified.com).

Garbage Cans. Although rarely considered security risks, garbage cans can serve as hiding places for contraband. See-through mesh designs, coupled with swift emptying, can reduce this risk. The Cincinnati Metropolitan Housing Authority invested in garbage cans and mobile "garbage vacuums" in 2008 to address these concerns, an approach that might be worth considering on some sprawling campuses ("Security Designed into New and Remodeled Facilities," Security Magazine, August 7, 2008, http://www.securitymagazine.com/CDA/Articles/Feature_Article/BNP_GUID_9-5-2006_A_10000000000000398690).

Related Resources

U.S. Department of Education, Office of Safe and Drug-Free Schools:

- *Practical Information on Crisis Planning: A Guide for Schools and Communities*, http://www.ed.gov/admins/lead/safety/emergencyplan/crisisplanning.pdf

National Clearinghouse for Educational Facilities (NCEF):

- *Mass Notification for Higher Education*, http://www.ncef.org/pubs/notification.pdf
- *Mitigating Hazards in Schools*, http://www.ncef.org/pubs/mitigating_hazards.pdf — information about hazard assessment, mitigation planning, and project funding.
- NCEF resource lists, *Access Control Systems in School and University Buildings*, http://www.ncef.org/rl/access_control.cfm, and *Campus Safety and Security*, http://www.ncef.org/rl/safety_securityHE.cfm
- NCEF Safe Schools webpage at the NCEF website, www.ncef.org

Public Alert Radios. NOAA Weather Radio All Hazards, a nationwide network of radio stations broadcasting all-hazards information 24 hours a day, 7 days a week. Broadcasts include alerts and safety steps for a wide range of emergencies and hazards, http://www.crh.noaa.gov/Image/lot/nwr/NWR-FactSheet.pdf

Publication Notes

First published May 2008; updated July 2008, October 2008, January 2009, April 2009.