School Security Technologies

National Clearinghouse for Educational Facilities

Tod Schneider
July 2010

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 backfire with power outages and technological failures. Some security technologies raise political and philosophical concerns. Still, technology, used correctly, can be highly functional and cost effective. Its pros and cons must be weighed carefully within the context of local sensibilities and conditions.

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 priority-ranking 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 suicidal or impulsive offenders, 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 technologies 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 codes dictate 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*.

Prepared under a grant from the U.S. Department of Education, Office of Safe and Drug-Free Schools

Lock-and-Key Systems

In many cases, a conventional lock-and-key system is still the best option. If it works, don't fix it. However, many schools readily admit that dozens of keys or more are floating around, lost, stolen or unaccounted for. If many keys have to be accounted for, checked out, and tracked, and this is spiraling out of control, look into a key management system that tightens control, or electronically establishes an audit trail showing who last checked a key out.

Indicators that conventional keys and locks are no longer adequate 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." Stamping should discourage duplication, although it is no guarantee that it will not occur.
- Lockdown plans that 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.
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.

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. Brigham Young University ((BYU) now uses access cards for all buildings.

There are a few basic down sides to electronic controls: initial cost, technical difficulties, and power outages.

Initial cost. If installation is integrated into the initial construction, it's likely to be more affordable than a retrofit, but in either case is considerably more than the cost of conventional lock hardware. Wireless technology may reduce installation costs. For example, Lehigh Career and Technical Institute (LCTI) in Schnecksville, Pennsylvania, used its existing WiFi network and compatible locksets to retrofit conventional doors campus-wide for centralized control without hard wiring (http://www.sargentlock.com/products/product_overview.php?item_id=1934). 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. If installing electronic door controls, consider installing data cabling at the same time, so that if you choose to install cameras at some point in the future, the wiring is already in place.

Technical difficulties. Someone has to install and run the software, updating information whenever a new card is issued or an 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 outages. All systems should have emergency back-up power. The alternative is complete systems failure during a 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 to 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 expire when the job is completed. Cards can serve multiple functions, acting as debit, library, attendance, 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. Jackson State students now use a combination of an ID number and biometric reader to gain access to dorms (Securitymagazine.com 5/10) Chiba Institute of Technology students, in Japan, log in to registration with a smart card and a palm reader. University of Georgia-Athens uses biometric hand geometry readers in dining rooms, the recreation center, and dormitories. It has also recently completed a pilot study on using biometric readers in exam sites. Bentley University, Mass., has used fingerprint readers on their laptops since August 2008. University of West Alabama, in Livingston, is using fingerprint readers, backed up by webcams, for on-line students, who must purchase and use the $180 devices to take tests. (Campus Technology May 2010 p.24)

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 his or her 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 the lockdown of a second door to prevent 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 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 $50,000 to $75,000 per revolving door or $13,000 to $45,000 per turnstile. 3-D image technology installed in the ceiling makes it much easier to identify piggybacking and sound an alarm (http://www.prosecurityzone.com/Customisation/News/Biometrics/Iris_Recognition/Iris_recognition_and_3D_image_sensing_anti-tailgating_system.asp).

Staff cooperation. Many security measures will fail if staff and students don't cooperate. For example, after shots were fired inside Wilson High in Virginia it became apparent that door security was being compromised. Students told reporters that they'd seen doors propped open with pencils, often for quite a while. The school now has hourly inspections. (*Student Safety May Get Public Forum*, Virginian-Pilot, May 23, 2010)

Visitor Screening and Badging

In most public schools, visitors don't receive access control cards, but they do receive visitors' badges 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. (One inspector reports that he often has signed into schools as "Charles Manson," without being questioned.) 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. Broward County Public Schools in Florida are using a Fast-Pass screening system that tracks people entering and exiting school sites. The system checks visitors against sex offender and law enforcement data bases, and confirms authorization for anyone picking up a child. It also screens volunteers as part of their application process. The system is networked to serve all buildings and entry points, and can serve to send district wide emergency messages to all work stations. A similar product at Paragon Charter Academy (http://paragon.heritageacademies.com/) serves as a "virtual security guard" — a machine that snaps visitors' photos and scans their driver's licenses, which are then run through national sex offender 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 an 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. In February, 2010, a Pennsylvania lawsuit alleged that school officials were activating school-issued laptop webcams while the students were at home. The district claims the devices were to be activated only if a computer was lost or stolen, for tracking purposes. Even in England, where cameras are commonly seen in public places, one private school created quite the storm in 2010 when they installed cameras in bathrooms to deter vandalism. (A hue and cry shut down the project before the cameras were activated.) On a pragmatic level, appropriately used cameras are merely affordable substitutes for placing staff members with better memories and an endless attention span in the halls to watch over our children, 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.

From deterrence and law enforcement perspectives, cameras are invaluable, and their use is spreading rapidly. For example, Oakland, California schools will be adding 750 cameras by August 2011, with footage linked to police for viewing as needed. About half the $3 million cost will be covered by a "Secure our Schools" DOJ grant. Over a five year period, from 2001-2006, arson attacks and vandalism that broke 600 school windows cost the Swedish city of Malmö about $6.5 million. In response they installed "smart" cameras. So far these have been an effective deterrent against recurrences.

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 studies have shown that people cannot focus effectively on electronic monitors for more than about 15 minutes at a time. 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 secured in opaque domes or similar enclosures that protect against vandalism without compromising the camera’s coverage area. Outdoor cameras may need heated or cooled housings for extreme weather. Cameras in corrosive, dirty, or extremely humid environments also can require protective housings. If components are going to fail, they are most likely to do so fairly quickly. Have spare components on hand for replacement purposes.

Wily criminals often can avoid cameras or wear disguises to obscure their identities. They also can attack the cameras as the first step in a planned crime. There are two measures that can be employed to outfox these offenders:

(1) Install cameras in overlapping patterns so that every camera is within the recorded view of another. In this way, any vandalism or tampering with one camera should be captured by another.

(2) It may be useful to have some covert cameras capturing images around the corner from the main viewing area, where offenders may not have yet donned disguises.

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 below.

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. Picture resolution is measured in pixels per foot (ppf). The minimum needed for facial recognition is 40 x 40, or 1600 pixels. License plate recognition starts at 6400 ppf. But 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. On the other hand, many institutions are already heavily invested in analog cameras and aren’t likely to replace them in the short

term. In those cases, hybrid systems, tying analog cameras into networked DVRs or other recording devices with higher-end processing capabilities can be a good solution — an approach recently used successfully at Georgia's Thomson-McDuffie Junior High School. Police can also tie into the system wirelessly, within 150 feet, for live video feeds. Unshielded twisted pair (UTP) wiring (CAT 5 or CAT5E cable) is an ideal transmission medium that should make it easier to eventually shift from analog to digital systems. In some cases, add-on devices (such as the VideoIQ iCVR Encoder) can upgrade analog cameras to function like smart cameras (discussed below), and this may be worth exploring as a less expensive upgrade option.

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 (e.g., www. immmervision.com, http://www.theiatech.com, or http://www.sentry360.com).

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, used by the Onondaga Central School District in upstate New York) will make these adjustments automatically.

Video analytics: specialized, "smart," or "intelligent video" cameras versus conventional equipment. Conventional cameras impassively collect images. Smart cameras can analyze "unusual behavior" in an environment, using 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. They can be triggered when equipment is removed from a room, and they can search all cameras for matching objects. Additional perimeter sensors become redundant if the cameras know what to watch for. Such "event-driven" video can trigger an alarm or tell a monitor to wake-up and display a live image. This will likely change the landscape of security offices — instead of walls of monitors, only one or two should suffice. Power and display space won't be wasted on pictures of empty hallways. Human on-site guard tours have some advantages — the high visibility of officers can deter misbehavior — but they are expensive, and a guard can only be in one place at a time. Attentive criminals will time their offenses to occur just after a guard or school resource officer has passed by and will predictably be absent for a period of time — or will make guards their first targets. With high end video analytics, one operator can manage 1,000 cameras, incidents are well documented, and claims of innocence or police brutality are much easier to address. When events do occur, video clips can automatically be sent to officers for a response on foot, or they can talk directly to the offenders through an integrated speaker system. It's important to note that, in at least one study, on-the-ground guards responding to alarms dramatically improved effectiveness in deterring thieves – with thefts in parking lots dropping 41 percent. Other public spaces using unsupervised, unmonitored, low quality cameras saw much more modest crime reductions (www.videoIQeye.com).

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. Improved digital signal processing (DS), low light sensitivity, and megapixel technology are boosting the ability to use edge devices for "video content analysis" (VCA). However, with so many analog cameras still in use, many institutions will need to handle the analysis at the head-end for some time to come.

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 — the 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 database 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. In addition to active processing capability, storage demands can be daunting: one megapixel camera can generate 207 gigabytes of data in 24 hours. Motion activation can help reduce the load, but retaining this kind of data for months or years adds up to a huge storage requirement. Creative storage arrangements can include off-site storage and information dispersal, with multiple back up copies, an approach that may be more cost effective than on-site storage.

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. Early systems recorded analog images onto reels of film that had to be developed before viewing. They 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 IP 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 below).

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 its network server. When purchasing components, it is essential to actually see not just the live image broadcast, but also the recorded image accessible after the fact and the printed result, field-tested on-site before finalizing a purchase. Focal length, equipment limitations, and weather can impact the quality of images generated, but lighting is a critical factor. The higher the number of megapixels, the more proper lighting is needed. Test any equipment being considered under low-light as well as changing conditions (day and night, rainy and clear).

Furthermore, whatever system you use must have a video management component, so that you can work with the data from all the cameras on your system. One example would be the CompleteView products from Salient Systems (www.salientsys.com).

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.

Mobile "push" technology. Automatic or on-demand delivery of images to mobile devices, such as Mobile Digital Terminals in police, security, or specialized emergency response vehicles (Mobile Incident Response Vehicles, or MIRVs, http://www.excelerate.info/home.aspx), or in some cases hand-held devices (such as iGuard, http://www.feelingsoftware.com/en_US/iguard-mobile-video-surveillance.html) can be invaluable as a resource for school resource officers or other crisis-response personnel.

Weapons Detectors

Another form of electronic surveillance is the metal detector, a device that 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 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 also will be needed, starting at about $30,000. Rather than reassuring students, however, 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 schools 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 that, if nothing else, motivates students to get to class on time. Battery life is short, so have back-up wands or batteries handy.

Communications

Everyone on campus should be able to call for help, pass along a timely warning, or receive a warning — anytime, 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 don'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 permit messages to be broadcast to multiple users simultaneously. Many devices now on the market combine multiple functions, such as the BlackBerry smartphones or the Motorola 8350i, which can include radio, cell, GPS, email and web services. 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 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. (For more information, see the NCEF publication *Selecting Security Technology Providers*.)

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 that area. 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. Alcatel's Omni-touch My Teamwork Land Mobile Radio Conferencing and Collaboration (LMRCC) platform, and Telesusa'sTalk Box each enable cross-frequency communication. The Talk Box is discussed in more detail in the NCEF publication *Mass Notification for Higher Education*. SchoolSafe provides a radio compatibility bridge — by clicking on an icon on a computer screen, emergency responders on exclusive radio bands can communicate directly with school staff on their much less expensive school radios (SchoolSafecom.org) . 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 (Plain Old Telephone Service, or POTS) in all classrooms and offices, for the moment at least, are still sound investments, although the time may be approaching when more economical models of routing, such as through an intranet or broadband system, may take over. (The FCC's vision over the next decade includes getting high speed broadband internet services into all anchor institutions, including schools.)

Teachers and students can rely on finding hard-wired phones 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. Some software now on the market transforms campus phones into loud speakers and ties a variety of communication options into one platform (Alcatel-Lucent OmniPCX Enterprise telephony network/ Safe Campus). Alcatel has developed a "911 snooping" technology, which automatically alerts campus security personnel to 911 calls and allows them to silently conference in, in order to coordinate with first responders. Indiana's Evansville Vanderburgh School Corporation provided portable VoIP telephones for all teachers. The phones are easy to move throughout the school, or to use on bus or playground duty. They can receive text messages and voice mail, which can also be retrieved from a computer. Using Singlewire Software's InformaCast, administrators can broadcast messages just to teachers, rather than using a PA system heard by the students. They also use blackboard connect for external messaging, such as messages home. The school has saved considerable money by eliminating most analog phone lines. (eSchoolNews May 10, p.29)

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). Most of the systems now on the market cannot distinguish between varying altitudes; in other words, they cannot determine if a call is coming from the first or fifth floor of a building.

■ At least one new product is addressing this, by installing $80 location nodes throughout a building. Users download SiteWERX software onto any bluetooth-enabled device to incorporate this feature, which lies dormant until 911 is dialed. The developer is currently working with half a dozen universities around the U.S.

■ The University of South Florida is trying out a new 911 service from Rave Wireless that allows users to submit information to a data base ahead of time, that will automatically be sent to a dispatcher if a 911 call is made. Information includes a photo along with addresses, phone numbers, emergency contact numbers, medical needs, or any other concerns.

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. For better or worse, kids' cell phone ownership has jumped dramatically – from 11.9 percent of kids 6-11 in 2005, to 20 percent in 2010. According to an MRI research study, ownership among 10-11 year olds has climbed over 80% during that period. Jon Akers, director of the Kentucky Center for School safety, wants student cell phones banned, claiming they "contribute to bullying, underachievement, sexual harassment and numerous disciplinary issues, cheating, and even criminal activity." (www.kysafeschools.org).

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 on radios, page 7).

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 that boost transmissions in dead zones. They are necessary because cell phones are much 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 operating 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. One alternative to satellite phones would be the GeoPro, which sends and receives text messages via IP and global satellite networks. It includes a built-in GPS, an emergency button, tracking, check-in, and waypoint functions. (www.geoprosolutions.com)

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. From a cost perspective, a mesh system may be more economical than the conventional approach of digging trenches and burying cables. Carnegie Mellon University addressed the problems of slow delivery and impenetrable walls with a customized system that delivers notifications to specific rooms or buildings 50 times faster than cell phones, by combining FM-bandwidth radio waves and mesh WiFi networking *(CampusTechnology August 2009, www.metissecure.com/products)*.

Incoming Message Options. Anyone with information about a potential threat should be able to reach school officials through multiple routes. They should be able to communicate anonymously or directly, by voice or text, by slipping a note into a tip box, or by slipping one under a door. Prominently display phone numbers or email addresses for this purpose. For a large district or municipality, a web-based tip service may be worthwhile, such as Speak-Up (www.paxusa.org) or tip411 (www.tip411.com).

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. Simple doorbells may be inexpensive additions that can be used along with existing cameras and remote locks to control visitors when the office has no direct view of an entry (an approach used at Abraham Baldwin Middle School, Guildford, Connecticut), or can be integrated along with a camera into an intercom device, such as an Aiphone (www.Aiphone.com). Rather than purchase and install an entirely new device, an alternative would be to integrate a new intercom feature into an existing smart surveillance system by running three new components to the camera: a doorbell button to an alarm input; an electro-magnetic door lock to the the alarm output; and a microphone and speaker to the audio jack (www.iqeye.com).

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.

Digital displays. In addition to individual text messaging and email systems, text-based digital display devices are becoming commonplace educational and emergency message distribution tools. Services such as RoomView® remote help desk (www.crestron.com) allow users to send messages to any text type device on a campus network, including whiteboards, projectors and displays, customized for a single room or broadcast across campus (also see the discussion in the NCEF publication *Mass Notification for Higher Education*).

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. Some now integrate LED signs, using customized visual messages to compensate for noise barriers to audio messages.

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. Detroit schools supplemented their existing alarm system with battery powered cameras that send 10 second video clips to the alarm monitoring station when alarms are triggered. (videofied.com)

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 his or her 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. Ohio State University is investing $1 million in an electronic tagging system that uses the school’s Wi-Fi network for tracking. They plan on installing $100 tags in 10-15,000 pieces of equipment between 2010 and 2012. The same technology may be used to track dementia patients, as well as employees who trigger personal wireless panic alarms. Children at risk of abduction could wear similar devices as well (www.ekahau.com/).

Self-initated emergency alerts. A number of applications can be added to cell phones, going beyond 911 capabilities, that allow individuals to call a number of resources for help as needed, such as friends, relatives, or campus security. One such product is Campus SOS link,™ which allows students to send alerts via Smartphones to selected individuals, with photos of the scene, their GPS location, text messages, and a follow up phone call (www.soslink.com) Another is Shadow me, which can be programmed to check on a user regularly, and send GPS information to designated recipients if there’s no answer (www.shadowmesecurity.com). Emergency alerts aren’t limited to cell phones either. Panasonic Classroom A+ Audio System combines classroom audio and camera systems with emergency features in a wireless infrared microphone. It is worn on a pendant, allowing the teacher to be heard clearly throughout the room. In an emergency she can silently send an alarm through the

pendant while triggering the video surveillance system. (PR Newswire 6/9/10).

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. For electronic devices, especially laptops, Lo-jack theft-recovery software can be downloaded (check sites such as Absolute.com or Gadgettrak.com). LAPD recovered 32 school laptops in 2009 using electronic tracking services. When the laptop is booted up within range of a wireless internet connection, it automatically sends word pinpointing its location. One product also uses built-in laptop web cams to snap pictures of suspects and send the jpegs along with the location and ISP address.

Low technology. When all else fails, be prepared to fall back on the basics, such as hand signals, flashlights, glow sticks, or floor level glow strips.

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 databases 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*.)

Integration and Convergence

Integration. Most large institutions have found value in tying all security components into a single platform in an IP-based 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. 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. But integrated systems need not be limited to security technology. Proximity cards are now commonly used not just for access control, but as debit cards in cafeterias, bookstores, copy shops or laundry rooms, for attendance, as library cards, and as storage devices.

Convergence. The biggest leap in this multi-faceted direction is known as convergence, which ties electronic (sometimes called “physical”) security into IT security (sometimes called “cyber” security) and data management. Institutions have become alarmed over the past decade at the astronomical growth in the theft or vandalism of intellectual property, as well as the invasion of privacy and exposure of confidential, proprietary information. Convergence ties everything together on a single platform. If workers are fired, not

only are their key cards deactivated, but their computer access codes are also immediately voided. As convergence has continued to evolve, the demand has increased for improvements in ease of use (often using on-screen maps and graphic user interfaces, or GUIs), efficiency and functionality for end-users. As much as possible these systems go beyond alerting security staff to incidents, analyzing situations and telling them precisely how to respond. This is sometimes referred to as a physical security information management (PSIM) system. A command and control platform ties together all system components and runs them through rules, workflows, and scenarios to guide the human operator. One example of such a platform is iView systems' iTrak Incident Reporting and Risk Management System, which ties together video, incident reports, risk analysis, visitor management, lost and found, employee databases, vehicle databases, and many more features (www.iviewsystems.com). A parallel development is the emphasis on converging security with non-security features, such as fire alarms, HVAC controls, lighting, power metering, phones, and sound systems, along with all kinds of data management and work flow, Automated reminders can be sent to all appropriate recipients, advising them about which employees are due for recertification, testing, or license renewal, for example. A converged system can identify students with excessive absences or failing grades, or who have overdue library books. Convergence eliminates costly redundancy and makes it infinitely easier to send information across silos and crunch data (see the Schools Interoperability Framework, or SIF, at www.sifinfo.org). Ave Maria University, in Naples, Florida, is a good example of total integration: they've tied together fire alarms, climate control, HVAC monitoring, access control, video cameras, low voltage lighting, electrical power metering, campus debit and security cards, voice-over-internet (VoIP), sound systems, LAN/WAN networks, wireless technology and more (Security Magazine 2009).

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.

IP Risks

A serious challenge with any IP-based device, converged or otherwise, is the possibility that the device, and by extension the network, can be compromised by hackers or viruses. In terms of IP-based operations, a dedicated, protected, virtual network is a safer way to go, shielded from equipment failure with redundant network computers. But this is not always an option. At any point where digital information is flowing through the internet, the risks are there. Eliminating the risk is not easy, because the demand for internet access is so strong. If schools don't provide wireless access, students and staff are likely to build their own pathways out of their own dorms or offices. A 2006 University of Iowa security audit found 80 rogue networks run by students and faculty members on campus. (eschoolnews.com 1/12/10). These rogue access points are Trojan horse superhighways for malware, viruses, information theft, snooping, and hacking of any kind. Default settings are usually wide open, allowing unrestricted access. The College of the Holy Cross, in Worcester, Massachusetts, addressed the rogue access point problem by using a program from Aruba Network that can search out and destroy student-enabled internet connections by scanning dorms for abnormal frequencies — a technique that can zero in on an unauthorized network within a few yards (eschoolnews.com 1/12/10). Ultimately, the best defense against rogue access points may be to meet the demand, so that students aren't tempted to create their own systems. Just bear in mind that digital vigilance is the price of internet freedom, which means Intrusion Protection Systems (IPS) are critical defensive tools against theft of intellectual property, malicious mischief, alteration of records, invasion of privacy, and viruses.

And it's not just computers that we have to worry about. When the Keller, Texas, Independent School District installed a wireless network that can stream high quality video to students' mobile devices, for anywhere anytime learning, they included a wireless IPS (WIPS) to guard against hackers. A diagnostic test runs daily to make sure the system's working school wide (eSchoolNews May 10, p.29). As William Jackson points out, "If it's got memory, it's got a processor, and it's on the network, it's a computing device" (GCNdaily 2/6/10). Indeed, computers and high tech phones are just the beginning. Other risks come with networked copiers, scanners, and fax machines, and the risks remain long after the machines are discarded. If they digitally store information on a hard drive, then anyone who parts out the machine has access to everything the machine has seen. And of course any intentionally portable storage device, such as laptops, CDs, or jump drives, are similarly vulnerable. For this reason, all of these devices need to be carefully tracked and controlled — a very daunting task.

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 the most.
- Do your homework. Research makes and models of equipment and seek out first-hand reports on 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

Student Training on Campus Shootings. Wayne State University, Detroit, Michigan, recently launched a one-hour on-line training for students on what to do if a school shooting occurs. The training was developed in response to lessons learned after a 2007 active shooter drill. In addition to realizing which technological changes and equipment were needed, it became clear that students needed to know how to stay safe.

Staff training. Radford University, in Virginia, offers Managed Awareness and Trust (MOAT) Training on safety and security to faculty, staff, and external vendors on all aspects of cyber security as well as campus safety, emergency preparedness, and related topics (www.awareity.com). Jenzabar's Retention Management Solution (RMS) provides software along with professional services to help identify at-risk college students and develop effective intervention strategies. (www.jenzabar.com)

Especially for stadiums. "SportEvac" is simulation software being funded by the DHS Science and Technology Directorate and tested by the National Center for Spectator Sports Safety and Security (NCS4) at the University of Southern Mississippi. The developers are creating virtual, digital 3D stadiums, filled with tens of thousands of avatars, programmed to react to crises as unpredictably as people. Once testing is completed at seven in-state schools, the software should become available nationwide, allowing security teams to cheaply and safely run through all kinds of crisis scenarios.

Resident Advisor Training. Magna Publications and the National Center for Higher Education Risk Management (www.ncherm.org) offer online courses for RA's on identifying and managing troubled students. (www.magnapubs.com/courses).

Fire Extinguisher Electronic Monitoring. The New Hampshire State House has installed devices which electronically monitor fire extinguishers as an alternative to monthly physical inspections. Some critics suggest such systems won't pick up various obstacles, corrosion, insect nests, etc. The en-Gauge fire-extinguisher monitoring system tracks location, functionality, age, in-service dates, history, inspections, and current pressure for each device. Removal of extinguishers triggers an alarm. Most new systems are wireless. Once the system is installed you can also monitor other devices, such as

defibrillators. Extinguishers with scalable wireless packages cost $300-500.

3D Surveillance Camera Enhancement software is now on the market that can be added to video management systems to create 3D campus maps in which camera images are seamlessly linked. This allows users to pan across different camera views without losing the context of the bigger picture (www.feelingsoftware.com/en_US/omnipresence-3d.html).

Integrated Lighting and Security Systems, put together by in-house electricians, is saving money for Liberty Mutual Insurance in their Boston headquarters. When employees use their prox cards to gain access, the system knows which lights on which floors will be needed, eliminating unnecessary lighting and making it easier for security staff to see which parts of the building are in use.

Wi-Fi equipped school buses tranquilize students. A mobile internet router on Vail, Arizona's, "internet bus" changed rowdy behavior into civility. Kids were too busy surfing or working on homework to pester each other (www.autonetmobile.com).

Energy saving applications are gaining traction as schools look for ways to trim budgets, especially while adding energy-using technologies. California State, Chico is using Power Save to manage network-based power usage on 800 lab computers, saving 23,000 kWh monthly. Power Save identifies computers sitting idle, saves open documents and shuts down the machine (www.faronics.com). Another application tracks power usage and politely advises the user of their efficiency, or lack thereof (http://www.greentrac.com/).

Contingency Planning. Many universities are now using lecture-capture technology to empower students to attend classes online when attending in person is unrealistic for any reason. This provides an easy Plan B avenue for business continuity — if an illness sweeps the campus, or inclement weather makes attendance unwise, students can be encouraged to stay home and attend classes electronically. Jackson State, George Washington University and Penn State College of Medicine are just a few examples of schools with such plans in place.

On the Horizon

WiFi to 4G "handoffs" are likely to become standard —eventually. Next-generation (4G) cellular (long term evolution, or LTE) technology and WiMAX (worldwide interoperability for microwave access) capabilities are both expected to become more available, as well as capable of "handoffs." What this means is if you are walking through campus and hit a spot where WiFi lacks coverage, your device may be able to seamlessly switch to cellular, and vice versa. In addition to greater convenience, this could reduce costs, because campus users could use WiMAX instead of using up costly cell phone minutes. As this evolves it will provide good motivation for having a WiFi system on campus, but only if it has integrated the new IEEE standards. Once that's the case, you will be well positioned for this handoff ability as devices catch up with the technology. The proliferation of wireless devices is expected to leap from 1.5 million in 2009 to almost 1 billion in 2019, according to IMS research (http://mobiledevdesign.com/hardware_news/expect-almost-one-billion-02192010/).

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). Meanwhile, a U.S. GAO study suggests that a number of key GPS satellites may fail in 2010, and technical and budget issues make it uncertain whether new Air Force satellites will be up and running in time to keep service uninterrupted.

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).

Cross-brand cooperation. The Physical Security Interoperability Alliance and the Open Network Video Interface Forum have been working for a number of years on establishing technology standards. The goal is to make it easy for different brands of equipment to talk to each other. This will make it easier for integrators to tie systems together, without customized software or equipment, and should reduce costs as a result.

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. The phones are intended to serve as "portable information kiosks," covering everything from class assignments and cafeteria menus to emergency messages. They also can 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]). Along similar lines, University of Maryland's Institute for Advanced Computer Studies has developed "V911," a new emergency alert technology for cell phones and PDAs, as part of MyeVye, which is still at the prototype stage. Students can push a button to directly link to campus police with their location, their identity and live video and audio. American University has instituted similar technology as well (www.Campustechnology.com, May 2009).

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).

In the meantime, most 911 centers are not yet positioned to deal with text messaging .This weakness was raised at the Association of Public Safety Communications Officials summit last winter. There is no indication of when the centers will be able to catch up with this technology.

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).

Cell phone add-on capabilities: smart phone chemical detection. NASA scientists are working on an iPhone-based gadget, "Cell-all," that detects harmful ammonia, chloride, hydrazine, formaldehyde, and other potentially harmful substances. Widely distributed, this would greatly expand detection capabilities beyond emergency workers to all cell phone users (Futuretense www.newsletter@americanpublicmedia.org). When it senses a chemical threat the phone alerts the user with a text message, vibration, noise or phone call. A large scale catastrophe will trigger a message sent to the nearest emergency operations center, with time, location and chemical information. The product is still in the prototype phase. The first version will sniff out carbon monoxide and fire using an "artificial nose," a piece of porous silicon that changes color in the presence of certain molecules.

Location Aware technology. *Check your cell phone to find out where your friends are located*. UW Madison Professor Jignesh Patel has developed an application that pinpoints users' real time locations for other users on a map. Emergency workers could use the technology to coordinate movements (www.locomatix.com).

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).

Trunked radio options may expand. The European trunked radio standard for Terrestrial Trunked Radio (TETRA) is being considered by the Utilities Telecom Council (UTC) for use in the U.S. If this occurs it will open up the U.S. market to a variety of new products and vendors. (Urgent Communications Tech Talk, June 17, 2009, Vol. 2 No. 21.

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 soon. 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 individuals based on characteristics such as clothing color and height ("A Post-Camera Society," Security Magazine, 8/12/08, 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," with one petabyte equivalent to 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"). But while many universities are shifting to cloud computing (the University of Arizona in Tucson, will be using it for staff email and calendars), K12 schools have been resistant, primarily for security reasons. Oregon may be one of the first to make the move, thanks to an arrangement between the Oregon Department of Education and Google to use the "Google Apps for Education" services. This includes email, calendars, online documents, video conferencing, and website creation. Oregon took ten months incorporating the system to allow time to ensure security features were in place.This cloud-based system could save Oregon about $1.5 million annually. Cloud computing gives managers more flexibility for adjusting scale and costs, and handling spike demands. Pooling computer resources across multiple schools or districts can reduce environmental impact and operating costs, and can be handled as capital expenditures or operating costs (Governing/ Andy Kim 5/3/1).

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, 5/9/08, 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). A low tech solution well worth implementing in schools is to simply empty the cans regularly, with particular attention to bathrooms, where many arsons occur. Removing the fuel reduces the likelihood of incidents.

***Defibrillators required*.** There's been a push for at least a couple years now to require defibrillators in schools. Oregon's SB 1033 requires each school campus to have at least one automated external defibrillator (AED) on or before January 1, 2015. The devices reportedly have already saved 13 individuals in Ohio schools.

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.

- Selecting Security Technology Providers, http://www.ncef.org/pubs/providers.pdf

- 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, July 2009, October 2009, January 2010, April 2010, July 2010. Written by Tod Schneider and edited by William Brenner.