Systematic, appropriate, and cost-effective application of security technologies in U.S. public schools to reduce crime, violence, and drugs

Mary W. Green

Sandia National Laboratories, Security Systems and Technology Center
Albuquerque, New Mexico 87185-0762

ABSTRACT

As problems of violence and crime become more prevalent in our schools (or at least the perception of their prevalence), more and more school districts will elect to use security technologies to control these problems. While the desired change in student and community attitudes will require significant systemic change through intense U.S. social programs, security technologies can greatly augment school staff today by providing services similar to having extra adults present. Technologies such as cameras, sensors, drug detection, biometric and personnel identification, lighting, barriers, weapon and explosives detection, anti-graffiti methods, and duress alarms can all be effective, given they are used in appropriate applications, with realistic expectations and an understanding of limitations. Similar to a high-risk government facility, schools must consider a *systems* ("big picture") approach to security, which includes the use of personnel and procedures as well as security technologies, such that the synergy created by all these elements together contributes more to the general "order maintenance" of the facility than could be achieved by separate measures not integrated or related.

Why security technologies?

The nature of being a young adult is that of experimentation and rebellion. However, young adults are not stupid; they will generally not try things if they know there is a high probability of being caught AND the consequences of being caught are fairly unpleasant. They will generally do whatever they can easily get away with. Therefore, **to reduce problems of crime or violence in schools, (1) the likelihood of being caught must be greatly increased, and (2) unpleasant consequences must be established and enforced.** Item (2) is, of course, a very social and political issue, and needs to be addressed head-on by school boards and communities across the country. This paper addresses item (1).

The ideal learning environment would provide a one-to-one ratio as in teacher-to-student, parent-to-child, or "Master"-to-"Grasshopper." With such undivided attention and guidance, few students would fail to thrive or would fall prey to the shenanigans of youth; all work would be done well, drugs would not be experimented with, etc. As this is impractical in our current culture, the ratio is forced closer to 25-to-1, or higher, especially when students are not actually in classrooms. This smaller amount of attention, unfortunately, allows students to be lost from us academically and socially.

The obvious solution is to provide for many more adults at the schools. Unfortunately, the cost of manpower (or of training/liability in the case of volunteers), can be impractical. And schools are learning what business and government facilities realized two decades ago: humans do not do mundane tasks well, manpower costs are always increasing, manpower turnover can make training costs skyrocket, and humans cannot always be trusted, which is totally unacceptable in a school environment. Hence the possible role of security technologies. Through technology, a school can introduce ways to collect information or enforce procedures or rules that they would not be able to afford (or rely on) adults to do. Technologies that can be considered for application in schools include cameras, sensors, drug detectors, breathalyzers, biometric and personnel identifiers, physical barriers, weapon and explosives detectors, and duress alarms.

The role of order maintenance

One additional consideration that cannot be overlooked is the perception of chaos on a school campus. If a school is **perceived** as unsafe, then "undesirables" will come in and the school **will become** unsafe. It is the "Broken Window Theory" on a much larger scale. It is, unfortunately, a *negative synergy* that allows seemingly insignificant incidents or issues to combine to provide the groundwork (or even just the reputation) of a problem school. This is why issues of

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

vandalism and theft can be almost as harmful at a school as actual violence -- they can create a breeding environment for the violence.

Therefore, issues contributing to an overall "order maintenance" must be taken seriously. Reducing theft, deterring vandalism and graffiti, keeping outsiders off campus, keeping the facility in good repair, getting rid of trash, and improving poor lighting are all paramount to a school. Technologies such as cameras, sensors, microdots (for identifying ownership), anti-graffiti methods, and biometric or other personnel identification techniques can contribute significantly in many school situations (but not all!), and should be considered as possible approaches to "order maintenance."

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

Anyone working in the security market is aware that there are literally thousands of products on the market, each claiming to be the "very best of its kind." And, unfortunately, there are a significant number of customers in the country who have been less than pleased with the ultimate cost, maintenance requirements, effectiveness, and operability of security technologies they have purchased. In the past, schools have quite often fallen into the category of unsatisfied customers, in that they are usually driven by finances to purchase the "lowest-bid" hardware and installation. Without becoming security experts themselves, it can be quite difficult for school administrators to always invest security dollars in the most appropriate ways.

At the same time, the application of these technologies must be cost-effective, maintainable, practical, and socially acceptable. Anyone can make a school secure using many impressive state-of-the-art technologies, given unlimited dollars, if there are no concerns of privacy, and no concerns exist about the impression that the school is some sort of prison. However, dollars ARE always limited, privacy IS a big deal, and few communities are going to accept a prison-like school for their youth. The issues come down then to applying security technologies where practical, effective, and acceptable. This is not a straightforward task.

A systematic approach to identifying the risks at a school

In the past, schools have rarely had the time or resources to consider their security plan from a *systems perspective* -- looking at the big picture of what they are trying to accomplish. Like any other type of facility, a school must understand WHAT it is trying to protect (its assets), WHO they are trying to protect against (the threats), and the general environment and operating constraints that they must work within (the characterization of the facility). (And this information may change from year to year, depending on the community and other factors.) Only then can any facility do an adequate job of pulling together a systematic approach to security, which will involve some combination of technologies, personnel, and procedures, and do the best possible job of solving its problems within its financial constraints.

[I would like to mention at this point that I have had the privilege of leading site surveys at a few of the nation's most high-risk facilities for the purpose of evaluating and making recommendations for security upgrades. However, I spent NO MORE TIME AND EFFORT in working with most of these facilities than I have in our recent work with a local high school. It is my observation that schools have a more difficult security job in some ways than many business or government facilities; their assets (kids) are large in number and enormously valuable, their potential threats (some of these same kids plus everyone else in the neighborhood) are uncountable, and their environment, which must be truly pristine in safety and security, must be open to the community. But school security budgets are low and their accountability to the public is high. THIS is a hard job! Now, this doesn't mean it costs as much to protect a school as it does a high-security facility, but it does require as much thought and careful planning.]

Characterizing a school's environment: Is the school new or old? Does everyone who ever worked at the school still have keys? Are gangs a problem in the area and do they bother kids at the school? Are the school grounds open and accessible to anyone or do fences or buildings restrict access? Are there many hiding places in the halls or classrooms? What is the nighttime lighting like? Is the school small enough so that most of the staff know most of the students and parents? What is the crime rate in the neighborhood? Does the sensor system work well or do the local police ignore the alarms due to a high false-alarm rate? Is the school administration well-liked by the students? Are teachers allowed access at night? Are students allowed off campus at lunch time? How many incidents of violence occurred at the school over the last three years? Are visitors forced to go through the front office before accessing the rest of the school? What is the "in" dress?

How much does the athletic program influence the rest of the student body? Are your most vocal parents pro-security or pro-privacy?

Defining a school's assets: For this school, and this school year, what is most at risk? Are the instruments in the band hall a very attractive target for theft or vandalism? Is the new computer lab full of the best and most sellable PCs? Of course, the protection of the students and staff is always at the top of the list, but the measures taken to protect them are driven by the defined threats.

Defining a school's threats: For this school year, who is your school threatened by? Gang rivalries? Violence behind the gym? Drugs hidden in lockers? Guns brought to school? Outsiders on campus? Drinking at lunch time? Vehicle break-ins? Graffiti in the bathrooms? Accidents in the parking lot? How sophisticated (knowledgeable of their task of malevolence) or motivated (willing to risk being caught or risk being injured) do the perpetrators seem to be? Measures taken to protect against these threats are driven by the characterization of the environment (the neighborhood) and the facility.

Through a good understanding of all of the constraints that your security plan must work within, and what potential threats and vulnerabilities are of most concern at the present time, the most necessary and effective security measures can be identified. If resulting designs (e.g., fencing, sensors, locker searches, speed bumps) are too costly or are unpalatable to the community, a school then has the justification for modification of the facility and facility constraints (e.g., back entrances locked from the outside, no open campus, no teacher access after 10:00 p.m., no lockers, etc.).

Designing the school security system

After identifying the vulnerabilities or concerns at most facilities, a systems approach to the security plan would then examine possible solutions to each vulnerability from the perspective of

Detection → *Delay* → *Response*

For any problem, it is necessary first to detect that an incident is occurring. For example, when someone is breaking into a building, it is necessary that this act be detected and that information be supplied to the authorities as soon as possible. Next, this adversary must be delayed as long as possible so that the response force may arrive (e.g., make it difficult for him to take stolen computers away from the facility quickly). One simple example would be to firmly attach (such as with bolts) computer components onto the large, heavy desks they sit on, so that a thief is forced to waste a lot of time to remove them. Lastly, someone must respond to the incident, such as the police force, to attempt to catch the thief.

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

Deterrence → *Detection* → *Delay* → *Response/ Investigation* → *Consequences*

The most appealing step in any school security system would be to convince the perpetrator that he shouldn't do whatever it is he is considering doing, whether it is perceived as too difficult, or not worth his while, or the chances of being caught are quite high. Unlike other facilities, where a perpetrator would be handed over to the authorities to deal with, a school often has the authority and/or opportunity to set the consequences for some incidents that occur on their campus. Indeed, these consequences can oftentimes be the deterrence needed to prevent many incidents. If a school made any student caught with alcohol on campus ALWAYS pull weeds on the athletic field for two Saturday mornings, students may be deterred from this particular act in the future.

To illustrate the application of this model, if one of the major concerns that the students have at their school is the alarming frequency with which cars are being broken into in the student parking lot, a model for the security system to address this concern might be:

Deterrence Erect signs that warn that the parking lot is under video surveillance.
Have a campus aide located at the parking lot whenever possible.

Detection Install video cameras (vandal-resistant) in the parking lot.
Send the video signal to a recorder for one-week archival.
If an incident occurs, examine that day's tape.

Delay Install 8' fencing around the outer regions of the parking lot, so that a perpetrator would be forced to get over this fence with stolen merchandise.
Close off the parking lot to vehicle traffic during the school day. (Make students with irregular schedules park in a separate area.)

Response/ Investigation Review tapes. Confront perpetrator with evidence (if a student) to elicit a confession.
Call authorities.

Consequences With evidence, enforce maximum consequences if possible. (This becomes additional deterrence for future.)

Obviously, this model is not appropriate for all aspects of security, but it serves as an excellent start when considering each problem or concern.

Evaluating a school's security-system design

In facilities with more resources, it is a reasonable exercise to run computer models to examine the effectiveness of most proposed security systems, especially those involving many layers of security, including both technologies and people. For a school, however, this is probably not reasonable. The next best thing to determine the effectiveness of a proposed security upgrade would be to get the opinions of as many appropriate parties as possible. Present the problem and then ask for comments on the proposed solution from the teachers, the student council, the parent advisory group, the local police, and other schools in the area. Making these groups a part of the security upgrade team also ensures buy-in and gets the word around that the school is taking active security measures (deterrence!).

The New Mexico School Security and Anti-Violence Program – PILOT

Sandia National Laboratories, funded by the Department of Energy's Education Outreach Program, and in partnership with the New Mexico Department of Education, Safe and Drug-Free Schools, the New Mexico Citizen's Crime Council, and the local Public Service Company, began a pilot project in January of 1996 as the beginning of the New Mexico School Security and Anti-Violence Program. The pilot school was Belen High School in Belen, New Mexico, about 30 miles south of Albuquerque. This school was chosen because it was viewed as a typical New Mexico school with average problems, because of the community support for such an endeavor, and because of its proximity to Sandia Labs.

The examination and analysis of Belen High School required very close interaction with and much work by the school principal, Ron Marquez, and the district superintendent, Michael Grossman. This analysis took approximately 100 hours of meetings and interactions over a four-month period. At the end of this analysis, a community meeting was held that included school administrators and school board members, the local police chief, the local sheriff, two district juvenile judges, the juvenile probation officer, the local state government representatives, city council members, the local newspaper, and a few teachers, students, and parents. Buy-in from this group was received for the general concept of ideas being considered for implementation at Belen High School. Reasonable concerns regarding privacy issues were discussed and resolved. Over the next month, eight classes were taught to eight different groups of interested students at Belen High School on various topics in security technologies, including sensors, cameras, and metal detectors.

By the sixth month of the project, all of the responsible parties had agreed to the set of security upgrades described below. The majority of this system was installed during the summer months and implemented when the students came back to school in September 1996. The hardware portion of this effort cost approximately $42,000.

Based on the vulnerabilities that Belen High School felt were of primary importance (which will not be listed here by request of the school), the following measures were included in the security upgrade to address six areas of concern:

Violence

- Provide a hand-held metal detector to the school for the rare occasions when a student needed to be searched or when there was news that a special event might involve weapons being brought to a school function.
- Install video cameras (vandal-resistant) in areas of concern on the campus. So far, we have had luck with the use of the "Silent Witness" camera.
- Install "black boxes" (similar to those used on school buses) in classrooms where requested by teachers. When a teacher is having a problem with a particular student(s), insert a camera at that teacher's request the night before and set to record during the problem times.
- Issue picture IDs to all students and staff; provide "fading" 8-hour temporary badges to the school to issue to all visitors on campus; post a security aide at the single campus vehicle entrance to check student IDs to get onto campus; require student IDs for students to attend athletic functions for free.
- Prohibit students from going to their cars during lunch time. Prohibit students from leaving athletic functions and then returning.

Theft/Vandalism

- Upgrade sensors in school buildings and classrooms, including wireless infrared sensors, glass-break sensors, and boundary-penetration sensors, especially in areas with large amounts of assets.
- Mark all attractive assets (e.g., computers, band instruments, hand tools, shop equipment, VCRs, etc.) in three different ways: (1) using indelible ink and stencils, mark "Belen High School" on all major surfaces, (2) hide "microdots" within equipment where possible to help identify stolen equipment which has had other markings removed, and (3) etch "Belen High School" on metal and hard plastic surfaces with an Air Scribe (by Chicago Pneumatic) which can still be identified even if the surface is sanded off.
- Install vandal-resistant cameras in the student parking area. Prohibit students from going to their cars during lunch time. Fencing will be installed by the school district next year. We have recommended an 8' chain-link with a small 1-1/4" mesh that deters easy climbing.
- Provide anti-graffiti sealer paints for those bathrooms that are usually hardest hit by graffiti.

Drugs/Alcohol

- Provide hair-analysis test kits for the detection of drugs to parents at their request. Results are provided only to the parents, who may then come to the school for help if desired.
- Provide a portable "breathalyzer kit" to the school for use in special situations.
- "Sniff" air vapor throughout the school using a new preconcentrator invented at Sandia Labs that is connected to an ion mobility spectrometer for the detection of drugs.
- Support the school in its decision to close the campus at lunch time and not allow students to go to their cars.

Safety

- Upgrade the parking lot lighting to improve safety for night-school attendees and evening athletic events.
- Install a fire alarm pull box in the cafeteria hallway which sounds a local alarm when the outside cover is opened, before the actual fire alarm system is pulled.
- Support the school in its decision to install speed humps every 50 feet along the main school road

Student and Teacher Buy-in

- Teach classes on security technologies to the Belen High School students.
- Present in-service workshops to the teachers to update them and gather feedback.
- Hire a Belen student to do some of the tasks and act as go-between with the student council.

Consequences

□ Provide support where needed to enable the school district and community to develop and enforce stronger consequences.

Early feedback

As of the writing of this document, the response to the security system upgrades has been extremely favorable. At the first parent/teacher group meeting of the new school year, a group of about 50 parents expressed their support for the new system, citing several anecdotes and incidents where their kids had already been influenced/affected by the system in a positive way. Break-ins in the student parking lot and fights on campus so far this year are averaging less than half of what they were the previous school year. Several procedural changes have also seemed to have had positive effects: the previous year, the hallways had been full of students skipping classes and wandering around. These students now have to show their student ID to campus security aides when challenged, and are then escorted to a study hall made to be more boring than class, and the hallways are now empty of students during class time.

Metrics will be gathered over the next two years at Belen High School to determine the long-term effects of the security system. While the early results would lead one to the assumption that the systems approach to school security is an excellent deterrent to many school problems, it must be realized that the security system is still in its "honeymoon period", and it will be very interesting to see if its deterrence effects last.

Lessons learned

(1) Every school, every year, is different. The different assets, threats, and environments of each school mandate that there is no single right way to do security in schools, and that the design of a school's security system will always be somewhat subjective until very detailed expert systems are created in the future.

(2) After working with many schools, it appears that the more risks you have at a school, the bigger price you are probably going to have to pay in terms of sacrificing personal rights and privacy to establish an acceptable level of security. Likewise, a school experiencing fewer problems is going to be able to enjoy more privacy to maintain that same level of security. The good news is that technologies can make this loss-of-privacy "more private". A person going through a student's pockets is probably a lot less palatable than a student going through a metal-detector portal.

(3) While most schools will identify the threat of weapons on campus as a major concern, very few of them are willing to commit to a realistic weapon-prevention program. Most of the measures necessary for such a program are extremely unpalatable and usually do not portray a desirable school image. Most schools will have to rely on the "order maintenance" and the deterrence provided by their security system.

(4) The work with Belen High School took us about 50% longer than we thought it would; schools need just about as much careful planning and coordination as some high-risk facilities.

(5) A school should try to minimize adopting technologies that require a great deal of expertise from an on-site expert; that expert will leave someday and oftentimes it is difficult to find someone else motivated enough to take over the responsibility.

(6) Include the local police department or response force in any security planning; they are critical to the school's goals.

(7) Small things can sometimes have the most far-reaching impact. Our use of ID cards seemed to have the biggest impact on the students and adults at Belen High School, yet from our analysis and models, the ID cards appeared less significant.

(8) It is SO much easier to design security into a school BEFORE it is built; a good design can greatly reduce the need for security technologies.

(9) Cameras in schools can be a really big deal to some people. A school should consult with its attorney before proceeding with a security approach that involves cameras, so that it will be well understood up-front what the limitations are.

Future work

At this time, Sandia National Labs is seeking funding from several federal agencies in order to create a series of handbooks for school administrators that would provide simple-to-use information on the various types of security technologies commercially available. These handbooks would include information regarding general costs for equipment purchase and upkeep, life span of the equipment, maintenance requirements, operational requirements, vulnerabilities, human-factor issues, and the most effective applications. It is also planned to include prescriptive information that a school administrator could use when going out for bid to potential vendors, rather than using "lists." For example, a request for bid for installing sensors in classrooms might require that "... the sensor system must alarm within one second of an intruder entering through any exterior or interior window, through any classroom door, or through any false-ceiling tile ...", rather than a "list" that calls for "... a motion sensor to be installed in each classroom ...", which allows too wide an interpretation by potential bidders.

Conclusion

At the rate security problems have been increasing in U.S. schools over the last 15 years, it is hard to imagine that public schools will be able to afford the liability they may incur in another few years. Schools will have to be more proactive in adopting the same precautions that any business adopts today in order to remain solvent. Security technologies can be a cost-effective and viable option for schools when applied systematically and appropriately, with the buy-in of all concerned parties.

Acknowledgments

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy.