Safety and Security Guidelines for K-12 Schools

from the

Partner Alliance for Safer Schools

April 2017
3rd Edition

Table of Contents

Executive Summary

School administrators must answer two basic questions when planning to implement security measures: What should we do? And how do we pay for it?

Since school officials are rarely experts in physical security, the answer to the first question is too often a haphazard combination of devices deployed in such a way that they never really become a security *solution*. This makes the second question more difficult to answer. A poorly designed system is an inefficient one, and this drives up costs while still failing to provide the desired level of security.

It is as if administrators were responsible for fire detection and suppression, but had no codes to guide them. How could they be expected to know what type of technology should be used, or even where to put alarms and sprinklers?

This document seeks to help school officials navigate the challenges associated with security equipment and processes. Developed by experts in the security industry, with extensive input from school officials and law enforcement, it:

- Analyzes school security threats
- Outlines the legal, moral and other arguments for making investments in security
- Examines the nature of risk, risk assessment and risk mitigation
- Explains the importance of having “layers” of security
- Offers specific recommendations for deploying security solutions

The recommendations, consistent with the practice of implementing security in-depth, describe approaches for various physical and technological “layers” in a school. Within each layer, the recommendations are divided into TIERS, progressing from TIER 1, which provides a good baseline level of security, to TIER 4, which includes the most aggressive approaches to securing a facility.

Many schools will not be able to implement the TIER 4 measures, and many have no need to do so. The general purpose of this guide and its TIERS is to provide school administrators with tools they can use to gauge their risk level, identify their security needs and, after factoring in available resources, develop a security plan tailored to their school that incorporates practices and procedures vetted by experts.

Given the wide variations among the nation’s schools, there is no such thing as a one-size-fits-all approach to security. Whether officials at a particular school determine that meeting the standards of TIER 1 would be best for their situation, or they identify risk factors that compel a move to other TIERS, this guide can help to inform their decision-making and provide an appropriate level of security for students and staff.

Foreword

Origins

In 2013, the Security Industry Association (SIA) launched a working group focused on identifying ways to enhance school security. The following year, SIA partnered with the National Systems Contractors Association (NSCA) to turn that group into a more robust organization that brought together members of the security industry, school officials and law enforcement to develop a coordinated approach to protecting K-12 students and staff. SIA and NSCA formed the Partner Alliance for Safer Schools (PASS) with the unified vision that combining their respective school safety programs, along with NSCA's mass notification and emergency communications task forces, would provide valuable insight and perspective. Their goal was to create a meaningful and powerful entity that would help schools – and their integrators – implement the most appropriate and effective security technologies.

Purpose

The PASS story is one borne out of concern for and commitment to school safety. PASS is dedicated to improving security and life safety in schools by leveraging the experiences and knowledge of stakeholders.

PASS focuses on addressing ongoing and emerging threats to students and educators, as well as providing education about vetted practices in security and life safety. Its role is to help both schools and the security and life safety industry manage the steps needed to make a real difference in this changing landscape by identifying:

- Guidelines for security technology applications
- Technological advances
- Skills-building opportunities
- Solutions to funding challenges

PASS' vision is to bring together a diverse group of experts to develop the best solutions for the complex security challenges faced by K-12 schools.

Guidelines

The job of a school administrator and school board member is both very rewarding and very difficult. The challenges faced on a daily basis with tight budgets, reporting requirements and accountability to parents and agencies requires a focused level of leadership that could vex the most seasoned CEO.

Administrators and teachers are responsible for helping to mold youth into productive citizens, and providing them with the resources they need to grow into successful adults.

The problems faced by administrators in the 21st century are different than those faced by their predecessors. This complicated environment – where discipline is difficult to enforce, liability (both personal and district) is substantial, and the safety of students is no longer the single purview of fire marshals and life safety experts – can leave administrators wondering where to find direction on issues related to school security.

PASS has a singular focus: To provide school administrators, school boards and public safety and security professionals with guidelines for implementing a tiered approach to securing schools.

PASS realizes that not every school system has the financial resources to invest in extensive security enhancements, yet they all face daily pressure to ensure that students are protected. This guide was produced to provide administrators with a means for measuring compliance with specific industry recommendations.

School safety, like educating children, is a long-term endeavor. The tiered recommendations in this guide are intended to provide a *general* overview of security needs for schools. Based upon local risks, as identified with the assistance of public safety and security professionals, administrators can focus on specific security enhancements that will provide the best return on investment.

As with many expenditures, budgets may force schools to phase in their solutions over several years. The tiered approach detailed in this guide can be used to gauge and determine phased goals for mitigating identified risks.

PASS realizes that deciding how to provide reasonable levels of protection for children is not just a matter of dry analysis; however, budgets are real, and unless a school has unlimited resources, difficult decisions related to how best to secure a school and its students must be made.

The guidelines identified in this document are not intended to provide solutions for every risk and every situation, nor to make product-specific recommendations. Administrators and public safety officials should work together, using this guide as a basis, to assess local needs and develop a risk mitigation strategy that is unique to their location.

A TIERED Solution

TIER: A row or layer in a series of similarly arranged objects. In a security

program, layers might be distributed among several tiers.

CONTINUUM: A continuous sequence in which adjacent mitigation elements are not perceptibly different from each other, although the implementation extremes can be quite distinct.

Traditional “best practices” may not work in the “tough choice” environment prevalent in America’s schools. For this reason, PASS has focused on detailing a TIER Continuum so that administrators can develop a plan to enhance security over time as budgets and resources allow.

In most circumstances, TIER 1 is a starting point. Collective discussions and input from public safety and security professionals can help administrators develop case study and budget justifications to move up through the TIER Continuum.

The ideas and recommendations detailed in this guide are meant to be “living.” When new risks are identified and new technical and operational approaches are developed, PASS will update the TIERS and general suggestions.

Introduction

Schools should be safe havens, places where parents can send their children without worry and where children can learn without fear.

For the most part, fortunately, that is the case. However, several horrific incidents have forced us to accept that there are exceptions, that absolute safety and security is impossible. The mass murders at Columbine and Sandy Hook, as well as fatal shootings at other schools, have led to reassessments of how we manage risk in the K-12 environment.

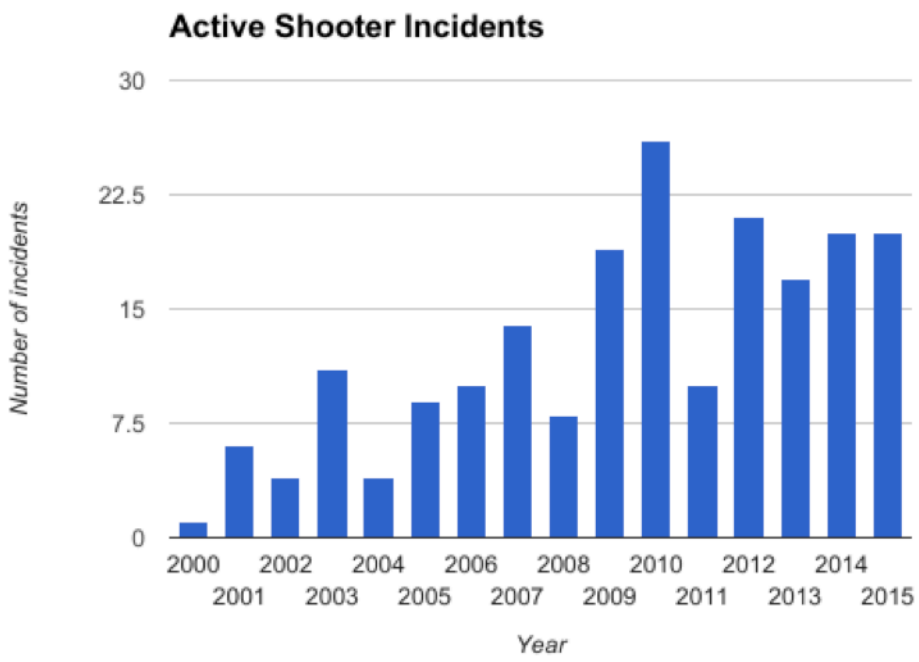
Active Shooter Incidents

From 2000 to 2015, the United States experienced 200 active shooter incidents, according to a pair of FBI reports from 2014 and 2016. These incidents resulted in 578 deaths and 696 wounded (excluding shooters).

Educational environments were the second-most common sites of active shootings during this time, with 45 occurring there, including 30 at K-12 schools. In those 30 shootings, 62 people were killed and 67 were wounded. In 13 of those incidents, the FBI reported, “unarmed principals, teachers, other school staff and students confronted the shooters to end the threat.”

“Recognizing the increased active shooter threat and the swiftness with which active shooter incidents unfold, these study results support the importance of training and exercises – not only for law enforcement but also for citizens,” the FBI stated in its report, *A Study of Active Shooter Incidents in the United States Between 2000 and 2013*. “It is important, too, that training and exercises include not only an understanding of the threats faced but also the risks and options available in active shooter incidents.”

It should be noted that compiling statistics on active shooter incidents presents challenges related to defining the term. The federal government defines an active shooter as “an individual actively engaged in killing or attempting to kill people in a confined and populated area,” and that is, with minor modifications, the definition that the FBI used. The bureau stressed that its statistics “do not encompass all gun-related situations; therefore caution should be taken when using this information without placing it in context.” For example, the data do not include shootings that resulted from gang activity or drug dealing, nor do they encompass suicides in public places or negligent discharges of weapons.



Source: *A Study of Active Shooter Incidents in the United States Between 2000 and 2013*, FBI, 2014, and *Active Shooter Incidents in the United States in 2014 and 2015*, FBI, 2016

Other Violence in Schools

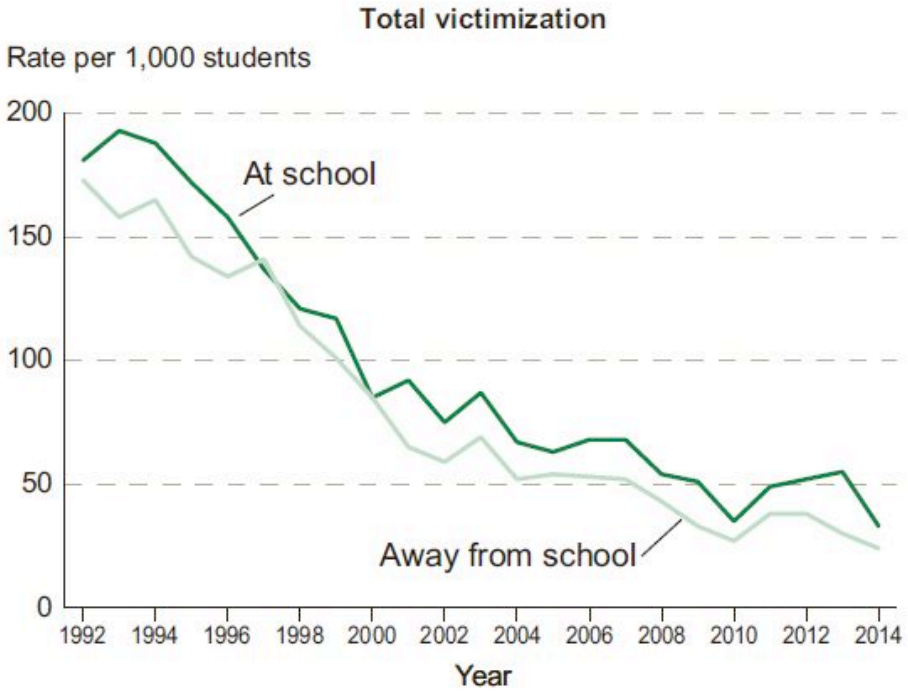
The extensive news coverage that active shooter incidents in educational institutions receive may create a misperception regarding their frequency. In a nation in which about 50 million students attend about 100,000 public schools, 30 incidents in 15 years is, thankfully, an extremely low rate. The threat cannot be ignored, but it should not distract school officials from other security concerns.

The National Center for Education Statistics and the Bureau of Justice Statistics reported in *Indicators of School Crime and Safety: 2015* that, among students ages 12-18, in 2014 alone, there were 486,400 "violent victimizations," ranging from simple assault to serious attacks including aggravated assault and rape. In addition, there were 363,800 "theft victimizations" during that year.

The active shooter statistics do not even fully cover all killings at schools. In just the one year between July 1, 2012, and June 30, 2013, there were 41 homicides in schools, including 31 of school-age youths (ages 5-18).

The good news is that the victimization rate in schools has decreased dramatically since the early 1990s, from 181 per 1,000 students in 1992 to 33 per 1,000 in 2014.

Still, though, in 2013, about 3 percent of students ages 12-18 reported being victimized in the previous six months, including 1 percent that reported being victims of violence. That same year, about 7 percent of high school students reported having been threatened or injured with a weapon while on school property. In addition, in 2011-12, about 1 out of 10 elementary and secondary school teachers reported having been threatened by a student.



Source: *Indicators of School Crime and Safety: 2015*, National Center for Education Statistics and Bureau of Justice Statistics, May 2016

Managing Risk

With hundreds of thousands of students being attacked each year, mitigating the risks associated with in-school violence is a major fiscal, legal and moral challenge for school officials. It requires careful planning, expert advice, and financial and other resources.

Even with the best policies, procedures and equipment in place, though, no facility can ever be 100 percent secure. Risk can never be eliminated, only managed. The sections that follow provide specific recommendations to school officials related to managing risk and enhancing security.

A Corporate Case Study for Security

What can school administrators learn from studying corporate security measures and protocols?

A school is not a corporation but, like any organization that invites people onto its property, a school system has a similar obligation to provide a reasonable level of security. Schools would do well to model their security approach after the corporate example.

Corporate America views security not as a reactive law enforcement function, but as a proactive security function that accomplishes the following:

- Based upon a documented assessment of the risk faced, a strategic alignment of security into daily operations resulting in a reasonable level of security for all people on the premises.
- A proactive approach to emergency management and loss prevention.
- An opportunity to generate positive public relations and community-focused goodwill.

These goals are admirable, but they hardly make a case for a significant investment in security. Corporations need more than “feel-good” justifications – they need a rationale. Given the tight budgets and multiple priorities faced by public schools, they need a rationale for the investment as well.

If the risk associated with an active shooter incident at any given school is statistically minimal, then why should a school allocate scarce resources to preventing such an incident?

The Rationale for Security Investments

As part of their mission statement, many corporations have a core value related to being a “good neighbor.” They want the public (i.e. customers) to view their involvement in the community as positively as possible. Corporations make investments of time, talent and resources to enhance their community reputation. In return, the community feels good about using (paying for) the corporation’s products and services. Part of this “good neighbor” investment is heightened security, but the cost for this security is difficult to justify without considering legal responsibilities and other measurable returns on investments.

Many corporations justify their security investments by looking at seven primary motivators for funding and maintaining a strong security presence:

- Moral and/or legal responsibility
- Liability reduction
- Controlling insurance costs
- Supporting economic health
- Public and employee relations
- Brand Protection
- Added value

All of these funding motivators apply to schools, and two have a particularly significant correlation to justifications for enhancing school security. For this reason, school administrators can learn valuable lessons from them as they fight for valuable resources.

Moral/Legal Responsibility

If an organization invites the public onto its facility, it has an obligation to reasonably manage its environment in such a way as to minimize the possibility of injury or death to invitees.

It is also the moral responsibility of an organization to take reasonable steps to preclude the destruction, misuse or theft of property so that the physical facility remains intact to carry on its business without interruption, and personnel are reasonably safe while conducting business (or education, in the case of schools) at the facility. This responsibility is owed to the parents and students who rely upon the service, the employees who rely upon a paycheck, and the taxpayers who support the facility.

Reasonableness is often defined by studying national trends and community norms. It should be remembered that school administrators at both the local and system level, as well as the school board, have a duty to the community to exercise care and skill in the management of affairs. This duty includes security management.

In regard to students, schools have an obligation that is contractual in nature: The organization assumes certain responsibilities toward students given the absence of parents during normal school hours.

Security and Liability

Liability reduction is a factor in many facets of security. If an organization is inviting the public onto its property, it has a duty to provide a reasonably safe environment. If this duty is breached and an incident occurs, possible financial liability could result.

A school is liable not only for the conditions of its facility, but also for its employees as well. A system may be held liable for the negligence of an employee to act (or fail to act)

in a “reasonable” manner under two controlling factors, as well as what may be termed community expectations based upon community norms.

Respondeat Superior (“Let the master answer”)

Respondeat superior is a legal doctrine stating that, in many circumstances, an employer is responsible for the actions, or lack of actions, of employees performed within the course of their employment.

What liability does a school system incur when threats have been identified and norms have been established, yet it fails to take prudent action to mitigate the risks and comply with the norms?

Corporate Negligence

In an educational environment, corporate negligence normally occurs when a school maintains its facility in a negligent fashion, furnishes defective supplies/equipment, hires incompetent employees or otherwise fails to meet accepted standards, and such failure results in harm or injury to a person to whom the system owes a duty.

Community Norms as Established Standards

When determining the level of security necessary at a facility, it is helpful to review the security at institutions of similar size that are located in areas with similar crime rates and risk factors. In short, if a school system fails to take certain steps to mitigate risks that have been taken by other schools in similar locations or with similar demographics and incident numbers, potential plaintiffs can cite the failure of that school system to, at a minimum, carefully consider taking similar precautions as a lack of adherence to industry standards and community norms.

NOTE: School systems are required to strengthen critical infrastructure security and resilience by the No Child Left Behind Act of 2001 and Presidential Policy Directive 21 (2013). Many individual states also require schools and public safety officials to develop partnerships and school safety plans. Administrators are encouraged to review their responsibilities with legal counsel.

Risk and Risk Exposure

Risk is generally defined as a “situation involving exposure to danger.” From a security and life safety perspective, the meaning of risk is incomplete without looking at “risk exposure.” Risk exposure relates to how one may “act or fail to act in such a way as to bring about the possibility of an unpleasant or unwelcome event.”

If schools fail to act, then they heighten their exposure to risk. But before detailing what acts they should take to mitigate risk, one must look at the risks to which schools are exposed.

Schools face the same risks as any other entity in society, especially those in which care for vulnerable persons has been placed in the hands of others. In this regard, schools have direct correlations with hospitals, geriatric facilities and daycare centers, with the closest link probably being hospitals. What are the specific similarities?

- Controlled environment with vulnerable areas
- Previous history of open access and a light touch with security
- Locations in high crime areas and along major thoroughfares
- Rural facilities making changes to match what have become de facto security standards (for hospitals: JCAHO, HHS and OSHA regulations)

Given the commonalities, should schools take steps to secure their facilities in a fashion similar to hospitals?

Exploring Risk

Risk knows no borders and respects no boundaries. While levels of risk vary, all facilities face similar hazards to one degree or another.

Several risks generally associated with hospitals are also faced by schools, including:

- Street crime (burglary, theft, assaults)
- Internal theft (employees, students, visitors)
- Compromise of confidential information
- Workplace violence (disgruntled staff, students, former students and former staff members, visitors, family members)

In addition to these general risks faced by hospitals, schools face other factors that can expose children to risk. These risks include, but are not limited to, the following:

- Parental custodial concerns
- Unsupervised visitors
- Gang activity
- Trespassing
- Bullying and harassment
- Community use of facilities
- Before and after-school programs
- Portable classrooms
- Open campus environments
- Vulnerability to kidnappers and sexual predators
- Disciplinary issues
- High-traffic and high-activity times, such as school opening and closing

In order to protect personnel and property, a comprehensive security plan should be established to mitigate these and other risks. The plan should include, but not be limited to, the following:

- Access control
- Perimeter Security
- Video surveillance
- Visitor access
- Emergency procedures
- Identification of staff and visitors
- Parking lot security
- Asset tracking and inventory control
- Ongoing training in security awareness and emergency preparedness

As a result of the involvement of law enforcement with many school systems, rudimentary pieces of a security plan may already be in place. The challenge is to pull these pieces into a usable and easily understood format that provides a guide for current and future risk concerns.

Risk Assessment

A risk assessment is the first step toward developing a comprehensive security plan. A risk assessment exercise involves defining the criticality and vulnerability of the asset being protected and then determining the probability of a loss. Some assets, such as people, proprietary information and electronic equipment, are more critical and deserve a more thorough review of their individual vulnerability.

Determining criticality and vulnerability are relatively straightforward missions. The concept of probability can be more difficult.

Determining probability involves an experienced review of trends. Conducting a trend analysis requires collecting data from a variety of public and private sources. The key to assessing this data is to begin locally, at the facility, and proceed to national trends. It is important to note that there is no way to reliably predict an incident. The goal of a school administrator should be to identify trends that might indicate an increasing probability of a particular risk.

The following can be used as a tool to help determine the probability of a security incident occurring.

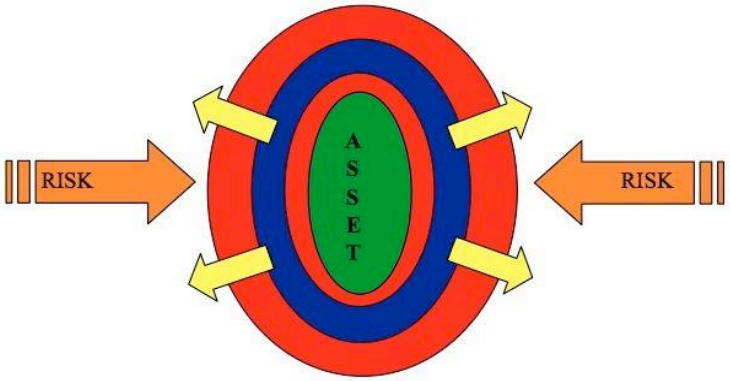
- Campus: Review incident report trends for at least 36 months.
- Area and city: Review crime data from local law enforcement for the surrounding neighborhood and city.
- Industry: Associations often provide information that can be used to quantify the risk associated with a particular facility based on national trends.
- Screening procedures: How is hiring conducted? While employees are generally screened for criminal records and drug use, are vendors and contractors screened at the same level? What about volunteers? Each negative response to these and similar questions increases both the risk and probability of a security incident.
- Anonymous tip lines: Enabling students, staff members, parents and the community to anonymously alert administrators to perceived and actual threats can help identify incident probability.
- Social media monitoring: No one likes the idea of “Big Brother” monitoring social media; however, in this era, when social media has been used to orchestrate social unrest and attacks, such monitoring can provide important information that can be used to identify risks.

There is no “crystal ball,” and risk assessment and mitigation can never be risk elimination. That is not to say, however, that risks cannot be identified, measured and reduced. Quantifying and mitigating risk are the jobs of security professionals and school administrators. The tools below can help them measure risk and prioritize their security investments.

Layers and Strategic Security

Strategic security provides a return on investment by becoming integrated into daily practices and protecting the school. To establish the parameters of the ROI, the level of security needed to protect the identified assets must be determined. In the case of schools, the primary assets are students and staff. Security parameters are established through a risk assessment using the established concept of layered security. (See Figure 1.)

Figure 1



Layers of security protect the asset from risks

The illustration above shows security layers. As one layer is bypassed, another layer provides an additional level of protection. Risk constantly pushes against these layers, looking for vulnerabilities.

Layered security works from the outside in. The asset being protected is at the center of the layers. Typical layers are detailed below.

Perimeter and Perimeter Barriers

Perimeter protection should deter or prevent those with criminal intent from entering the campus. Perimeter barriers may include patrols, fencing, guard houses, shrubbery, sidewalks, access control, lighting and other physical and psychological barriers.

Exterior

The exterior layer typically includes the parking area, walkways and access points into a facility. This layer also includes security patrols and lighting.

Interior

Interior security consists of compartmentalizing departments and areas according to their security sensitivity.

Procedural

The procedural layer involves the security management plan and specific departmental policies. This layer of the plan would detail patrol standards and documentation, response to unauthorized entry attempts, gate controls and other matters.

People

Personnel (vigilant staff and security) are arguably the most important component of each layer. To visitors and other guests, vigilant staff appear to be highly customer-driven. To those with criminal intent, their vigilance is an effective deterrent.

Technology

Technology includes, but is not limited to, video surveillance, duress alarms, access controls and notification systems.

Classroom Barricade Devices

Some school systems are incorporating classroom barricade devices into their security plans. These devices, when deployed, prevent a door from opening.

While they could be effective in keeping out an active shooter, such devices often violate fire codes, life safety codes and the Americans with Disabilities Act. In addition, the possibility that a violent student who is in a classroom could use such a device to prevent staff or first responders from entering could put students at greater risk. Active shooter incidents are extremely rare, but other violent acts are not uncommon in schools. As a result, making these devices available in classrooms might exacerbate risk, rather than mitigate it.

The 2015 *Final Report of the Sandy Hook Advisory Commission* stated, “The testimony and other evidence presented to the Commission reveals that there has never been an event in which an active shooter breached a locked classroom door.” PASS opposes the uses of classroom barricade devices and recommends the door control measures described in the “Classroom Layer” TIERS below.

The PASS position statement on this issue can be viewed at www.passk12.org.

Cybersecurity

Security equipment, more and more, is going online, with digital video cameras, access control equipment and, even, intrusion alarms being connected to the Internet. The networking of security solutions offers valuable new functionalities, such as analytics and remote access, but it also brings about new risk, primarily in the form of hacking and ransomware.

Security solutions should be implemented in close consultation with IT staff. School officials must ensure that their staff adhere to good cybersecurity practices, such as:

- Replace default passwords with strong passwords
- Implement policies and procedures for detecting and responding to breaches, both attempted and successful
- Regularly update software and firmware to install security patches
- Default to HTTPS
- Periodically audit networks
- Segregate/compartmentalize networks, as appropriate
- Securely back up data on servers that are not connected to the same network or in the cloud

This list is, by no means, complete. Countless resources on cybersecurity are available, including a “Beginner’s Guide to Product and System Hardening” from the Security Industry Association, which is attached to the end of this document.

Developing a Security Plan

Given all of the above, what can a school administrator do to enhance security in both the short-term and long-term?

The best answer involves TIERS of security. Security measures are not an "all-in" proposition. If they were, every facility would be protected like Fort Knox. Based upon both the identified risk (demographics, location, local crime rate, etc.) and funding availability, administrators can TIER and/or phase in their risk mitigation efforts.

By identifying a given school's TIER, administrators have the ability to communicate the facility's security status to the school board and parents as they seek support in advancing up the TIER continuum, as necessary.

PASS is not suggesting that every school and every security layer should be at the highest TIER; rather, the TIERS are provided so that administrators, parents, school boards and law enforcement professionals have a guide for measuring a school's vulnerability. As part of developing localized security solutions, PASS encourages school officials to assess their risk and determine the appropriate TIER within each layer. Simply thinking about security in a holistic way is a significant step toward mitigating risk.

PASS does recommend that schools adopt a long-term perspective with their security solutions. Whenever possible, schools should attempt to lay a foundation that will allow progression from one TIER to another.

NOTE: Except where otherwise noted, each TIER includes all recommendations in the preceding TIER(S).

TIER Continuum: Procedural Layer

The human element is critical and is detailed in several of the layers. Schools should work with local public safety and other experts to fully develop the human element of risk mitigation. As schools assess their risk and work on mitigation efforts, the roles and responsibilities of staff, teachers, volunteers, administrators and law enforcement should be documented and made an official part of the school system's policies and procedures.

TIER Continuum: Drill Layer

NOTE: As schools develop their internal policies and procedures and advance up the TIER continuum, they should work with local and state officials to develop plans for drilling students, staff and law enforcement on active threat scenarios.

TIER 1

A. School administrators should work with local and/or state law enforcement to identify specific active threats and implement active shooter training.
B. For both drills and actual emergencies, schools should have maps available that show room numbers, closet details, camera locations and locked doors for emergency responders.

TIER 2

A. All recommendations in TIER 1.
B. Schools should conduct annual “tabletop” exercises with teachers and law enforcement that mimic the actions necessary when facing an active threat.

TIERS 3/4

A. All recommendations in TIER 2.
B. Schools should conduct annual live drills that simulate active threat scenarios and that involve law enforcement, firefighters, students, staff and parents.

TIER Continuum: Property Perimeter Layer

TIER 1

A. The property perimeter should be clearly defined with signage stating that entry onto school property is limited to authorized visitors and those on official school business.
B. Exterior lights should be installed at strategic points on the property perimeter and should illuminate the area during periods of darkness so that unauthorized and criminal activities are more easily recognized.
C. The school property should be clear of debris. Trees, shrubs and other growth should be cut back to minimize interference with lines of sight throughout the property.
D. School employees and volunteers should be trained to immediately question anyone on school property, even at the furthest perimeter point, who does not have a visitor’s pass and is not accompanied by a school official.

E. Unauthorized use of school grounds by outside groups or individuals for basketball, soccer, football, skateboarding or other activities should be strictly prohibited, and violators should be prosecuted for trespassing.

TIER 2

A. Gates should be installed at all drive entrances or at other strategic drive “choke points” to allow school officials to effectively lock down the perimeter after regular business hours. This practice discourages the use of school property for unauthorized and/or illegal activities.
B. Law enforcement should be encouraged to have patrolling officers confront and, as appropriate, arrest trespassers.

TIER 3/4 (any combination of the items below)

A. Electronic access gates should be installed at each entry with intercom voice communication to the front office for vehicle entry.
B. As appropriate, and after an assessment determines it is proper to do so, gates can be left open during school drop-off and pick-up times.
C. Fencing or impenetrable shrubbery should be installed around the school property to discourage unauthorized entry.

TIER Continuum: Parking Lot Layer

TIER 1

A. Signage that clearly directs visitors, staff, students and delivery drivers to authorized parking areas should be installed at all entry drive points.
B. The bus drive should be clearly marked and segregated from other drives during periods of student loading and unloading.
C. Exterior lights should be installed at strategic points and should illuminate the parking lot during periods of darkness so that unauthorized and criminal activities are more easily recognized.
D. Staff members should be trained to confront any vehicle not parked in an authorized area.

TIER 2

A. Parking decals, stickers or numbered hang tags should be provided to staff members and regular volunteers, and prominently displayed on their vehicles.
B. Routine walk-through patrols of the parking lot should be scheduled throughout the day. Patrol members can be culled from the administrative team, office staff, custodians and parent volunteers.

TIER 3

A. A parking lot attendant, whose primary responsibility is patrolling the parking areas and school perimeter and watching for unauthorized and/or suspicious activity, should be hired.
B. The parking lot attendant should be provided with a radio and trained in personal safety and confrontation strategies by an appropriate professional.

TIER 4

A. Staff and volunteer parking areas should be gated with access cards.
B. License plate recognition technology should be installed at all controlled entrances in order to control unauthorized vehicle entry and aid post-incident investigations.

TIER Continuum: Building Perimeter Layer

NOTE: PASS does not recommend, nor approve of, keeping doors between buildings unsecured; however, practical limitations related to existing buildings and the flow of students can make it very difficult to secure all perimeter doors. This is especially true at a high school. All perimeter doors should be secured when students are in classrooms or when access from the exterior is not required for students to move from building to building. Teachers can be trained to unlock/dog these doors during class changes, or electronic access measures can be used to facilitate class changes and other access needs (at higher TIER levels). Exterior doors should comply with appropriate building codes, IBC, NFPA 80, NFPA 101 and NFPA 730 requirements for fire, life safety and security.

Perimeter doors are installed for free exiting of the building in the event of a fire or other emergencies that require evacuation of the building. These doors will generally have panic exit hardware installed on them. The most secure is called a “rim exit device.” A rim exit device is a locking device that keeps the door secure while allowing free egress from the building as required by life safety codes. Typically, these devices will not have a handle or other means to open the door from the exterior. If the door is needed for entrance into the building, the door should have a cylinder and pull handle that allow a key to be used to unlock and open the door from the exterior. These devices should have a visual indicator so that security and building personnel can look at the device and determine if it is in a secure condition. Exit devices should allow for dogging (putting into an unlocked state) only by means of a key. The second type of locking device is a lockset (if egress codes do not require panic exit hardware). These locks should be storeroom function (outside trim always locked). Preferably, there would not be an outside lever – just a cylinder to access and some type of vandal -resistant pull.

Keys should be of the patented type, and should not be able to be duplicated without following a formal authorization process controlled by the school.

Doors used for class changes between buildings should be monitored as closely as possible. Teachers in classrooms located in the vicinity of these unsecured doors should be trained to monitor the entry points.

Where remote release is suggested in the guidelines, it shall be by means of electric latch retraction for exit devices or electric locks. Use of electric strikes is not recommended.

If there is any error in installation positioning, the lock is easily defeated.

Signage should be placed on every door indicating that all visitors must sign in at the front office. Individuals attempting to enter without authorization are subject to arrest.

Exterior lights should be installed at strategic points on the building perimeter, illuminating the area during periods of darkness so that unauthorized and criminal activities are more easily recognized.

TIER 1

A. All exterior doors not routinely used for class changes should be secured with a working mechanical lock or exit device as required by codes.
B. All entry doors should be clearly marked with the first responder door and window numbering system to ease identification of entry points during emergency or tactical situations. Numbers should be made of reflective material similar to the numbers on a mailbox. In addition, the number system should be clear to the first responder as to where the door/window is within the relation of the school. For example, labeling a Door 1 of 21 or 1-21, allows first responders to decide which direction to go to find a specific door/window. Most first responders request the door/window labeling begin at the main entrance and proceed clockwise from the main entrance.
C. The main (visitor) entry should be visually monitored by a staff member or volunteer at all times during the school day.
D. The staff member monitoring the door should have a direct line of sight to the walkway leading up to the door, in addition to the door itself.

TIER 2

A. All exterior doors, including those used to go from one building to another during class changes, should be secured with a mechanical lock or exit device as

required by code. Doors may be unsecured ("dogged down") during class changes (at the bell).

B. Students needing access to another building should be escorted by a staff member, parent, volunteer, or other adult.
C. The main (visitor) entry should be secured with a mechanical lock or exit device as required by code and a doorbell. Anyone requiring entry during regular school hours should ring the bell.
D. A staff member or volunteer would then assess the request. If no overt threat exists, he or she would then physically open the door.

TIER 3

A. All recommendations in TIER 1 and recommendations in TIER 2, A and B.
B. The main (visitor) entry should be secured with an electronic access control device, video intercom, and remote door release.
C. Exit devices shall operate with electric latch retraction (electric latch retraction is when the latch bolt, which puts the door into a locked condition, is retracted, allowing the door to be opened). They shall have internal latch bolt monitor switches to indicate the position of the latch bolt (this indicates whether the door is locked). Power transfers should be concealed to avoid tampering. Doors should be provided with concealed door position switches. Door and latch position should be monitored at a central monitoring station.
D. Anyone requiring entry during regular school hours should request entry via the intercom. A staff member or volunteer would then assess the request and, if no overt threat exists, electronically open the door.
E. Electronically releasing the door should momentarily interrupt the door position and latch bolt monitor alarms.
F. Local alarm should be placed in the vicinity of the door to alert nearby classrooms of a security breach immediately.

TIER 4

A. All recommendations in TIER 3.
B. All exterior doors used by students for class changes and movement between buildings should be secured with an electronic access system that allows for scheduled lock/unlock times.
C. Doors used for student movement between buildings at times other than class changes should be designated, with access made available via temporary issuance of access cards and/or video intercom door release systems.
D. Bullet-resistant glass or film is recommended for exterior sidelites and doorlites complying with NFPA recommendations.
E. A secure vestibule should be built that separates the main entry doors from the actual building interior, and/or an entry door into the main office should be

installed that is separate from the secured entry into the school.

TIER Continuum: Video Surveillance Layer

NOTE: A video surveillance system is a key component of any security program. While direct lines of sight can enhance the safety of the school, a working video system is an excellent deterrent, assists in investigations and can be used by law enforcement in tactical situations. While many analog video systems are still in use, it is the opinion of PASS that new installations should be specified with IP cameras as a fully networked system. When existing analog systems reach their end of life, or when funding becomes available, analog systems should be retrofitted with a full IP system.

Further, the video system should follow the guidelines detailed below:

1. All cameras should record in full color.
2. Interior cameras should be mounted at the door looking down the hall so that a full-face shot of any person leaving the school with a child is more readily available.
3. The camera system should be checked daily, with documentation detailing the status of the system as a whole and individual cameras, identified problems, and steps taken for problem resolution.

It is very important to note that, in video surveillance, there is no such thing as a "one-size-fits-all" approach. Designing a quality video surveillance system can be complicated and requires a collaborative approach using multiple professionals, including an integrator and a consultant. School administrators should be familiar enough with the terminology and video technology that they are able to make an informed decision. To this end, PASS has supplied a glossary of video terms at the end of this guide.

TIER 1

A. A video surveillance system should be installed that covers, at a minimum, the main entry exterior, front lobby, main office and student pick-up/drop-off lane.
B. This video system should be installed by a properly trained, manufacturer-certified installer, in accordance with state and local codes.
C. The video system should have the capability and flexibility to expand to meet the guidelines of the subsequent video surveillance TIERS.
D. The video system mission-critical equipment (recording devices, power supplies, etc.) should be in a secured location, such as a locked closet.
E. The video system should be connected to the school's network so that it is capable of being remotely accessed by authorized personnel, including first responders during emergency and tactical situations.

F. The video system should be capable of storing archived video for a minimum of 14 days.
G. At least four people at a given school should be trained on and capable of using the system for surveillance and/or investigations, and to assist law enforcement in a tactical situation.
H. The video system should have the capability to export historical incidents for forensic review.

TIER 2

A. Video coverage of all common areas, such as the cafeteria, gym, media center and theater, should be provided.
B. Video coverage of all exit doors, facing from the door down the hall, should be provided.
C. Video coverage of strategically important exterior areas, such as the drives on and off campus from the main building, the bus lane area, and walkways from portable classrooms to the main building entry, should be provided.
D. A wall-mounted public view monitor should be installed at the front entry and/or the main office so that visitors can "see" themselves as they enter the school. NOTE: The public view monitors should *only* show the feed from the main entrance camera.
E. The minimum storage capability of the video system should be increased from 14 to 21 days.

TIER 3

A. Video coverage of restroom entries and stairwells should be provided.
B. Staff member(s) should have the camera system on a dual monitor during regular business hours so that video is always displayed.
C. The minimum storage capability of the video system should be increased from 21 to 28 days.

TIER 4

A. Video coverage of all halls and cross halls and the full building exterior should be provided.
B. Video coverage of high-liability risk areas, such as in-school suspension rooms and alternative education rooms, should be provided.
C. The video surveillance system should be monitored by a district security operations center and/or the local law enforcement dispatch center.
D. The video surveillance system should be integrated with mobile applications to enhance situational awareness during an event.

TIER Continuum: Visitor Control Layer

TIER 1

A. The school should utilize a sign-in system for visitors that is controlled by a staff member or volunteer. The sign-in book should document the visitor's name, address and reason for visiting the school.
B. The staff member or volunteer should verify the accuracy of the provided information by checking it against the visitor's government issued identification.
C. Central office administrators should audit visitor process compliance and work to ensure that all schools in the district handle visitors in a consistent manner.
D. Visitors should wear a self-adhesive visitor's pass that is unique to a given school in color and/or design.
E. The visitor's pass should have a "date valid" and day of the week notation that is large enough to be seen by an average-sighted person from a distance of 3-4 feet.

TIER 2

A. Recommendations in TIER 1, B-E.
B. The school should utilize a computer-based sign-in system for visitors that is controlled by a staff member or volunteer. The sign-in software should document the visitor's name, address and reason for visiting the school, and should print a visitor's pass.

TIER 3

A. All recommendations in TIER 2.
B. The sign-in system should automatically check the visitor's name against a national sex offenders registry. NOTE: Consult local law enforcement and legal representatives to determine the best approach to handling anyone found to be on the registry.

TIER 4

A. All recommendations in TIER 3.
B. All parents and authorized visitors (including vendors, contractors, etc.) should be pre-enrolled in an electronic identity-based system before the school year begins.
C. All visitors should present a government issued credential upon arrival that is scanned to initiate the sign-in process so that the visitor can be matched against the pre-enrolled database.
D. If the visitor has not been pre-enrolled, the sign-in system should automatically check the visitor's name for local warrants. NOTE: Consult local law enforcement

and legal representatives to determine the best approach to handling anyone found to have a warrant.

TIER Continuum: Classroom Layer

While technology and other equipment may be targets, the most important assets in a classroom are students, staff, and visitors. Other TIER continuums detailed in this guide, such as video surveillance and emergency notification, will serve as protective layers for the classrooms. The TIERS listed below relate to securing the classroom door against active threats, unauthorized visitors, and criminals. Schools should work with first responders, local law enforcement, and EMS to coordinate how access is gained to classrooms under the various TIER levels listed below.

TIER 1

A. Classroom doors should be lockable from the inside by means of a push button. Push button locks allow locking of outside lever without the use of a key, and do not require the teacher or staff member to step out into the corridor. (Note: This allows anyone to be able to lock the outside lever, which may have unintended consequences.) Locks are keyed on corridor side for access by authorized personnel.
B. Classroom doors should have a window so that administrators and other adults can see what is happening inside at any time. Glass should be bullet resistant or have bullet resistant film applied to it according to NFPA 730.

TIER 2

A. Classroom doors should be provided with classroom security locks that require a key to lock from the inside. (Note: This limits the locking of the door to authorized personnel who have a key.) Locks are keyed on corridor side for access by authorized personnel.
B. Locks shall have a visual indicator. From the interior of the room, the condition of the lock (locked or unlocked) is visible to room occupants.
C. If a key is required to lock the door from the inside, teachers and other staff members should be trained to always have the key on a wrist or an over-the-head lanyard.

TIER 3

A. Classroom doors should be equipped with a standalone electronic door lock that can be locked wirelessly from a fob or other device from anywhere in the classroom.
B. Locks shall have a visual indicator. From the interior of the room, the condition of the lock (locked or unlocked) is visible to room occupants.

C. Locks are keyed on corridor side and have credential access by authorized personnel.
D. Teachers and other staff members (in the classroom) should be trained to always have the fob or activating mechanism on a wrist or an over-the-head lanyard.

TIER 4

A. Classrooms should be equipped with electronic locking systems that can be initiated both remotely or by a teacher in the classroom. This is a networked solution tied into the school security system.
B. Locks shall have a visual indicator. From the interior of the room, the condition of the lock (locked or unlocked) is visible to room occupants.
C. Locks are keyed on corridor side and have credential access by authorized personnel.
D. Teachers and other staff members (in the classroom) should be trained to always have the fob or activating mechanism on a wrist or an over-the-head lanyard.
E. Staff (not in a classroom) should be trained on how to activate the lockdown system.

   NOTE: PASS recommends that school administrators work with local life safety experts to determine code compliance related to securing classroom doors.

TIER Continuum: Emergency Notification Layer

TIER 1

A. A public address system should be installed that allows the front office to communicate to the school as a whole and, as necessary, to particular wings/areas of the school.
B. Custodial and other auxiliary staff members should be trained to verbally communicate to areas that are not covered by the public address system, such as gyms, portable trailers, etc.
C. Staff members should be trained to call 911 in an emergency using either an office line or a personal cell phone. Staff should be trained to never assume that someone else has called 911.
D. A phone/intercom system equipped with E-911 should be installed so that anyone can dial 911 without a passcode or number to get an outside line.

TIER 2

A. A “duress” or “panic” button should be available to office staff that alerts local law enforcement of a significant security incident in which an immediate response is necessary.
B. A wired or wireless duress button should be available in every classroom.

C. Staff should be trained on the location and use of the duress button, and should test the connection monthly.
D. A two-way communication system connecting each classroom to the front office or other central location should be in place.
E. Teachers, coaches and others who take students outside for recess, physical education and outdoor classrooms should carry and have access to two-way radios.

TIER 3

A. The duress system should have the capability to create SMS alerts for appropriate personnel and computer pop-up messages on local PCs, as well as central office PCs.
B. The duress system should provide independent and automated alerts to local law enforcement and other first responders.
C. Consideration should be given to installing duress buttons in hallways and other common areas, with the potential benefits weighed against the possibility of false activations.
D. Staff should be trained on the location and use of the duress buttons and should test the connections monthly.
E. The public address system should meet NFPA-72 ECS requirements for intelligibility including pre-recorded messages.

TIER 4

A. The duress system should have the capability to generate a camera stream with the computer pop-up message so that responding personnel (law enforcement and school administrators) can see a live view of the area where the duress button was activated.
B. The public address system should be integrated with fire alarms, weather alerts and the duress system to automate emergency messaging that provides information as to what the emergency is, what to do and where to go, and that sends an “all clear” message when appropriate.
C. The public address system should be augmented through the use of digital signage that provides emergency information.
D. The public address system should be integrated with the two-way radio system used by security personnel, law enforcement and firefighters so that calls for emergency response are automated.
E. The two-way communication system should be able to accept calls from emergency personnel outside the building.

Closing

While the TIERS detailed in this guide provide a baseline approach for securing a school, the recommendations are not intended to be all-inclusive.

This guide is meant to be a first step toward open communication and discussion between administrators, law enforcement, parents and security professionals. Communication is key to understanding and developing support for security efforts.

PASS welcomes feedback about these guidelines. Questions and comments may be submitted on the group's website at www.passk12.org.

Glossary

Establishing a solid security foundation for a school requires administrators to work with various security industry professionals, including information management teams, security consultants and engineers, security systems integrators and manufacturers. Many of the terms used by these professionals are foreign to most administrators. This glossary is provided to help lower the language barrier and assist administrators in making informed decisions about their security solutions.

Video Surveillance Terms

Angle

The field of view, relative to a standard lens in a 35mm still camera, expressed in degrees. For practical purposes, this is the area that a lens can cover, where the angle of view is determined by the focal length of the lens. A wide-angle lens has a short focal length and covers a wider angle of view than standard or telephoto lenses, which have longer focal lengths.

Aspect Ratio

A ratio of width to height in images. A common aspect ratio used for television screens and computer monitors is 4:3. High--definition television (HDTV) uses an aspect ratio of 16:9.

Bit Rate

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but it actually defines the number of bits/time unit and not distance/time unit.

Codec

In communications engineering, a codec is usually a coder/decoder. Codecs are used in integrated circuits or chips that convert (e.g., analog video and audio signals into a digital format) for transmission. The codec also converts received digital signals back into analog format. A codec uses analog-to-digital conversion and digital-to-analog conversion in the same chip.

Codec can also mean compression/decompression, in which case it is generally taken to mean an algorithm or computer program for reducing the size of large files and programs.

DHCP (Dynamic Host Configuration Protocol)

DHCP is a protocol that lets network administrators automate and centrally manage the assignment of Internet Protocol (IP) addresses to devices in a network. It uses the concept of a “lease” or amount of time that a given IP address will be valid for a computer. The lease time can vary, depending on how long a user is likely to require the network connection at a particular location. DHCP also supports static addresses for computers running web servers, which need permanent IP addresses.

DVR (Digital Video Recorder)

A DVR is the device in which video from a camera is recorded. A DVR works much like a VCR tape, except it uses a hard drive to store the video. Typically, a DVR is directly connected to a video surveillance camera. A single DVR can be connected to up to 32 cameras.

Ethernet

Ethernet is the most widely installed local area network technology. An Ethernet LAN typically uses special grades of twisted pair wires. The most commonly installed Ethernet systems are 10BASE-T and 100BASE-T10, which provide transmission speeds up to 10 Mbps and 100 Mbps respectively.

Focal Length

Measured in millimeters, the focal length of a camera lens determines the width of the horizontal field of view, which is measured in degrees.

FTP (File Transfer Protocol)

FTP is an application protocol that uses the TCP/IP protocols and is used to exchange files between computers/devices on networks.

Frame Rate

The frame rate used to describe the frequency at which a video stream is updated is measured in frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Gain

Gain is the amplification factor and the extent to which an analog amplifier boosts the strength of a signal. Amplification factors are usually expressed in terms of power. The decibel (dB) is the most common way of quantifying the gain of an amplifier.

GOV Length

The GOV length determines the number of images (VOPs) in the GOV structure.

H.264

Also known as MPEG-4 Part 10. This is the compression standard for digital video. H.264 offers higher video resolution than Motion JPEG or MPEG-4 at the same bit rate and bandwidth, or the same quality video at a lower bit rate.

H.265

This is a powerful compression standard that will replace H.264.

HDTV (High-Definition Television)

HDTV provides up to five times higher resolution than standard analog TV. HDTV has better color fidelity and a 16:9 format. The two most important HDTV standards today are SMPTE 296M and SMPTE 274M, which are defined by the Society of Motion Picture & Television Engineers (SMPTE).

HTTP (Hypertext Transfer Protocol)

HTTP is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the web. The HTTP protocol runs on top of the TCP/IP suite of protocols.

HTTPS (Hypertext Transfer Protocol over SSL)

HTTPS is a web protocol used by browsers and web servers to encrypt and decrypt user page requests and the pages returned by the server. The encrypted exchange of information is governed by the use of an HTTPS certificate (issued by a certificate authority), which guarantees the authenticity of the server.

Interlacing

Interlaced video is video captured at 50 pictures (known as fields) per second, of which every two consecutive fields (at half height) are then combined into one frame. Interlacing was developed many years ago for analog TV and is still used widely today. It provides good results when viewing motion in standard TV pictures, although there is always some degree of distortion in the image.

To view interlaced video on a computer monitor, the video must first be de-interlaced to produce progressive video, which consists of complete images, one after the other, at 25 frames per second. See “Progressive Scan.”

IP (Internet Protocol)

IP is a method of transmitting data over a network. Data to be sent is divided into individual and completely independent “packets.” Each computer (or host) on the Internet has at least one address that uniquely identifies it from all others, and each data packet contains both the sender’s address and the receiver’s address. IP ensures that the data packets all arrive at the intended address. As IP is a connectionless protocol, which means there is no established connection between the communication end-points, packets can be sent via different routes and do not need to arrive at the destination in the correct order. Once the data packets have arrived at the destination, another protocol - Transmission Control Protocol (TCP) - puts them in the right order. See “TCP (Transmission Control Protocol).”

IP Address

An IP address is simply an address on an IP network used by a computer/device connected to that network. IP addresses allow all the connected computers/devices to find each other and pass data back and forth. To avoid conflicts, each IP address on any given network must be unique. An IP address can be assigned as fixed so that it does not change, or it can be assigned dynamically (and automatically) by DHCP. An IP address consists of four groups (or quads) of decimal digits separated by periods, e.g. 130.5.5.25. Different parts of the address represent different things. Some part will represent the network number or address, and some other part will represent the local machine address. See “IP (Internet Protocol).”

IP Camera

The terms IP camera, network camera and Internet camera all refer to the same thing: A camera and computer combined in one unit. It operates as a standalone unit and only requires a connection to the network.

Infrared (IR)

Infrared radiation is radiation at a longer wavelength than visible light, which means it cannot be seen by the unaided human eye. As infrared radiation can be detected as heat, this can be shown on a screen or captured by a digital camera, with hotter objects showing up brighter against colder surroundings (e.g. a human body against a colder background).

Inputs/Outputs (I/Os)

The digital I/Os on, for example, a network camera can be used to connect any device that can toggle between an open and a closed circuit. If, for example, a door switch is used as an input device, opening the door could trigger the upload of video images and

the sending of notification messages. An output might, for example, be used to automatically start a siren when there is a motion detection trigger.

JPEG (Joint Photographic Experts Group)

Together with the GIF file format, JPEG is an image file type commonly used on the web. A JPEG image is a bitmap, and it usually has the file extension ".jpg" or ".jpeg." When creating a JPEG image, it is possible to configure the level of compression to use. As the lowest compression (i.e., the highest quality) results in the largest file, there is a trade-off between image quality and file size.

kbit/s (kilobits per second)

A measure of the bit rate, i.e., the rate at which bits are passing a given point. See "Bit Rate."

Lux

A standard unit of illumination measurement.

MAC Address (Media Access Control Address)

A MAC address is a unique identifier associated with a piece of networking equipment or, more specifically, its interface with the network. For example, the network card in a computer has its own MAC address.

Mbit/s (Megabits per second)

A measure of the bit rate, i.e., the rate at which bits are passing a given point. Commonly used to give the "speed" of a network. A LAN might run at 10 or 100 Mbit/s. See "Bit Rate."

Minimum Illumination

The smallest amount of light needed for the camera to produce an image of useable quality. Minimum illumination is presented in lux (lx), which is a measure of illuminance. In general, provided it is not overexposed, the image will be better the more light that is available in the scene. If the amount of light is insufficient, the image will be noisy or dark. The amount of light that is required to produce a good-quality image depends on the camera and how sensitive it is to light.

Motion JPEG

Motion JPEG is a simple compression/decompression technique for network video. Latency is low and image quality is guaranteed, regardless of movement or the

complexity of the image. Image quality is controlled by adjusting the compression level, which, in turn, provides control over the file size and, thereby, the bit rate. High quality individual images from the Motion JPEG stream are easily extracted. See “JPEG.”

MPEG (Moving Picture Experts Group)

MPEG develops standards for digital video and audio compression. It operates under the auspices of the International Organization for Standardization (ISO). The MPEG standards are an evolving series, with each designed for a different purpose.

MPEG-4

MPEG-4 is a group of audio and video coding standards and related technologies. The primary uses for the MPEG-4 standard are web (streaming media) and CD distribution, conversational (videophone), and broadcast television.

Most of the features included in MPEG-4 are left to individual developers to decide whether to implement or not. This means there are probably no complete implementations of the entire MPEG-4 set of standards. To deal with this, the standard includes the concept of “profiles” and “levels,” allowing a specific set of capabilities to be defined in a manner appropriate for a subset of applications.

Multicast

Technology that reduces bandwidth usage by simultaneously delivering a single stream of information to multiple network recipients. See “Unicast.”

NVR (Network Video Recorder)

An NVR is a network device, typically a server, that receives video from IP video surveillance cameras throughout the network. It records the video images to hard drives. The main difference between a Digital Video Recorder (DVR) and an NVR is that an NVR is not directly connected to the camera.

Some NVRs are considered “hybrid” devices. A “hybrid” NVR is a device that has a video surveillance camera directly attached to it and that also receives video from IP cameras through a network connection. See “DVR (Digital Video Recorder)”

ONVIF (Open Network Video Interface Forum)

ONVIF is an open industry forum for the development of a global standard for the interface of network video products.

Pixel (Picture Element)

A pixel is one of the many tiny dots that make up a digital image. The color and intensity of each pixel represents a tiny area of the complete image.

PoE (Power over Ethernet)

PoE provides power to a network device via the same cable that is used for the network connection. This is very useful for IP surveillance and remote monitoring applications in which it may be too expensive or impractical to power the device from a power outlet.

Progressive Scan

Progressive scan, as opposed to interlaced video, scans the entire picture, line by line, every sixteenth of a second. In other words, captured images are not split into separate fields as in interlaced scanning.

A computer monitor does not need interlacing to show a picture on the screen. Instead, it shows the picture progressively, one line at a time in perfect order, i.e., 1, 2, 3, 4, 5, 6, 7, etc. There is virtually no “flickering” effect. In a surveillance application, this can be critical when viewing detail within a moving image, such as a person running. A high-quality monitor is required to get the most from progressive scan. See “Interlacing.”

Protocol

A special set of rules governing how two entities will communicate. Protocols are found at many levels of communication; there are hardware protocols and software protocols.

Resolution

A measure of how much detail a digital image can hold; the greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 320x240.

Alternatively, the total number of pixels (usually in megapixels) in the image can be used. In analog systems, it is also common to use other format designations, such as CIF, QCIF, 4CIF, etc.

Router

A device that determines the next network point to which a packet should be forwarded on its way to its final destination. A router creates and/or maintains a special routing table that stores information on how best to reach certain destinations. A router is sometimes included as part of a network switch.

SSL/TLS (Secure Socket Layer/Transport Layer Security)

These two protocols (SSL was succeeded by TLS) are cryptographic protocols that provide secure communication on a network. SSL is commonly used over HTTP to form HTTPS, which is often used on the Internet for financial and other sensitive transactions where security is needed. SSL uses public key certificates to verify the identity of the server. See “HTTPS (Hypertext Transfer Protocol over SSL).”

Switch

A switch is a network device that connects network segments together and that selects a path for sending a unit of data to its next destination. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route. Some switches include the router function. See “Router.”

TCP (Transmission Control Protocol)

TCP is used with IP (Internet Protocol) to transmit data as packets between computers over the network. While IP takes care of the actual packet delivery, TCP keeps track of the individual packets that the communication (e.g., a requested web page file) is divided into. When all packets have arrived at their destination, it reassembles them to re-form the complete file.

TCP is a connection-oriented protocol, which means a connection is established between two endpoints and is maintained until the data have been successfully exchanged between the communicating applications. See “IP (Internet Protocol).”

Unicast

Communication between a single sender and a single receiver over a network. A new connection is established for each new user. See “Multicast.”

VMS (Video Management Software)

VMS is the interface that is used for a network video recorder (NVR) to connect to and store video from an IP camera, as well as the user interface for people to view live and recorded video.

WEP (Wired Equivalent Privacy)

A wireless security protocol, specified in the IEEE 802.11 standard, which is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to that usually expected of a wired LAN. Security is at two different levels: 40-bit and 128-bit encryption. The higher the bit number, the more secure the encryption.

WPA-PSK (Wi-Fi Protected Access - Pre-Shared Key)

This wireless encryption method uses a pre-shared key (PSK) for key management. Keys can usually be entered as manual hex values, as hexadecimal characters, or as a passphrase. WPA-PSK provides a greater degree of security than WEP.

Emergency Communications Terms

ACU (Autonomous Control Unit)

The ACU is the main component of the ECS that connects to the devices used to initiate a live or prerecorded voice message and the audible and visual notification devices. The ACU monitors whether an initiating device or notification device is not working and alerts the building occupants of problems with the system.

ADS (Acoustically Distinguishable Space)

A room, hallway or any enclosed area in which an emergency communication message is announced. An ADS is determined by the shape, size and sound characteristics of the room. An ADS space must meet certain intelligibility requirements. See “Intelligibility.”

AHJ (Authority Having Jurisdiction)

The organization, office or individual responsible for approving equipment, materials, installations or procedures regarding emergency notification systems. Generally, this is the local or state fire marshal.

Alarm

A signal or message from a person or device indicating the existence of an emergency or other situation that requires immediate attention.

AOR (Area of Rescue) System

A two-way emergency communication system used for communications between first responders (fire or police personnel) and building occupants. AOR systems are typically installed in areas where building occupants would go if they are unable to evacuate the building. Examples include stairwell landings, storm shelters and elevator lobbies.

CIS (Common Intelligibility Scale)

A method for measuring a voice communication to test whether it is intelligible. See “SII (Speech Intelligibility Index).”

Combined Emergency Communications Systems

Various emergency communications systems, such as fire alarms, mass notification systems, elevator communications and others that can be served via a single control system or through the interconnection of several control systems.

DRMNS (Distributed Recipient Mass Notification System)

DRMNS is a system that is meant to communicate directly to targeted individuals and groups who might not be in an area covered by the emergency communication system. Emails and text messaging are examples of DRMNS. Also known as “mass messaging.”

E-911 (Enhanced 911)

E-911 is the general term referring to emergency telephone systems with specific electronically controlled features, such as dialing 9 to get an outside line.

ECS (Emergency Communication System)

A system that indicates the existence of an emergency situation and that communicates information needed to facilitate an appropriate response and action. See “MNEC (Mass Notification Emergency Communication).”

Emergency Response Plan

A documented set of actions outlining the responses to be taken in event of natural, technological or man-made disasters and other emergencies.

EVAC System (In-Building Fire Emergency Voice/Alarm Communication System)

A dedicated manual or automatic device for originating and distributing voice instructions, as well as alert and evacuation signals, pertaining to a fire emergency to the occupants of a building. EVAC systems are generally understood to be for fire alarm notification only.

FACI (Fire Alarm Control Interface)

A device that connects the fire alarm system with the emergency communication system (ECS) so that, in case of an emergency, the fire alarm system can be silenced so that a voice communication can be made.

HPSA (High Power Speaker Array)

An HPSA includes large speakers that are part of a wide-area mass notification system (WMNS). Typically, these are mounted on a pole or on top of a building to provide voice messages to a large outdoor area. See “WMNS (wide-area mass notification system)”.

Initiating Device

Any device that activates the emergency communication system (ECS) to broadcast a live or pre-recorded message is considered an initiating device. Initiating devices include

pull stations, emergency push buttons, a local operating console (LOC), computer-based software alerting tools, and mobile applications.

Intelligibility

Intelligibility is generally defined as a measure of how understandable a voice communication is.

LOC (Local Operating Console)

A telephone-like device that allows emergency personnel to make a live or pre-recorded voice announcement across an emergency communication system (ECS). LOCs are generally located in areas such as a facility's main office, near the front door, and near a fire alarm control panel.

Lockdown

A procedure used when there is an imminent threat in a facility. Personnel are secured in the rooms they are currently in, and no one is allowed to leave until the situation has been resolved. It is most commonly implemented when a building has an intruder.

Lockout

A procedure that allows no unauthorized personnel into a building. All exterior doors are locked, and the main entrance is monitored. This allows for the continuation of normal activities with a heightened level of security. It is most commonly used when an incident is occurring outside a facility.

Mass Notification Layers

Emergency communications used for mass notification are categorized into layers related to the audience to be reached:

- Layer 1 relates to notification of occupants by systems and equipment installed inside a building. See "ECS (Emergency Communication System)."

- Layer 2 relates to notification of occupants outside a building. See "WMNS (Wide-Area Mass Notification System)."

- Layer 3 relates to notification of personnel through individual measures. See "DRMNS (Distributed Recipient Mass Notification System)."

- Layer 4 relates to notification of personnel by public measures (broadcast radio, television, etc.)

MNEC (Mass Notification Emergency Communication)

MNEC refers to emergency communication systems, in general, encompassing WMNS (Wide-Area Mass Notification System), DRMNS (Distributed Recipient Mass Notification System), etc.

MNS (In-Building Mass Notification System)

A system used to provide information and instructions to people in a building or other area using voice communication and also including visible signals, text, graphics or other communication methods.

NAC (Notification Appliance Circuit/Network)

A network of devices used for transmitting emergency communications throughout a building and an area. The devices may include, but are not limited to, loudspeakers, horns, visual signals (strobes), HPSA (high power speaker arrays), and digital signage displays.

One-Way Emergency Communication System

A system that broadcasts information to people in one or more specified indoor or outdoor areas. Brief emergency messages are conveyed by audible, visual or textual means, or any combination thereof.

Paging System

A system intended to page one or more persons by such means as voice-over loudspeaker, coded audible signals or visual signals, or lamp annunciators. Paging systems are not considered emergency communication systems.

Risk Analysis

A process used to characterize the likelihood, vulnerability and magnitude of incidents associated with natural, technological and man-made disasters and other emergencies.

STI (Speech Intelligibility Index)

A method for measuring a voice communication to test whether it is intelligible. See “CIS (Common Intelligibility Scale).”

STIPA (Speech Transmission Index - Public Address)

A method for measuring the intelligibility of voice communications for emergency communication systems.

Shelter-in-Place

Personnel within a building remain where they are until given further instructions. It differs from a lockdown in that room doors are not secured and movement within the building is not restricted.

Two-Way Emergency Communication System

Includes both systems to be used by building occupants and systems to be used by firefighters, police and other emergency services personnel. Such systems are used to communicate information such as, but not limited to, instructions, acknowledgement of receipt of messages, environmental conditions, and the condition of personnel.

WMNS (Wide-Area Mass Notification System)

A system that provides real-time information to outdoor areas and may have the capability to communicate with other nearby notification systems.

References

NOTE: The documents below are a sampling of some of the resources produced recently regarding school security and active shooter incidents.

Centers for Disease Control and Prevention, "Youth Risk Behavior Surveillance - United States, 2013" (2014): http://www.cdc.gov/mmwr/pdf/ss/ss6304.pdf?utm_source=rss&utm_medium=rss&utm_campaign=youth-risk-behavior-surveillance-united-states-2013-pdf

Council of Educational Facilities Planners International, "Safe Schools - A Best Practices Guide" (2013): http://media.cefpi.org/SafeSchoolsGuide.pdf

Electronic Security Association, "Electronic Security Guidelines for Schools: An Aid for Schools Considering Procurement of an Electronic Security System" (2013): http://c.ymcdn.com/sites/www.esaweb.org/resource/resmgr/ESA-Resources/Guidelines_-_School_Security.pdf

Fantz, Ashley, Lindsey Knight and Kevin Weng, "A Closer Look: How Many Newtown-Like School Shootings Since Sandy Hook?" CNN.com (June 19, 2014): http://www.cnn.com/2014/06/11/us/school-shootings-cnn-number/

Federal Bureau of Investigation, "Active Shooter Incidents in the United States in 2014 and 2015" (2016): https://www.fbi.gov/file-repository/activeshooterincidentsus_2014-2015.pdf/view

Federal Bureau of Investigation, "A Study of Active Shooter Incidents in the United States Between 2000 and 2013" (2013): http://www.fbi.gov/news/stories/2014/september/fbi-releases-study-on-active-shooter-incidents/pdfs/a-study-of-active-shooter-incidents-in-the-u.s.-between-2000-and-2013

National Association of School Resource Officers and National Association of School Psychologists, "Best Practice Considerations for Schools in Active Shooter and Other Armed Assailant Drills" (2014): http://www.nasponline.org/resources/handouts/bp_armed_assailant_drills.pdf

National Center for Education Statistics and Bureau of Justice Statistics, "Indicators of School Crime and Safety: 2015" (2016): https://nces.ed.gov/pubs2016/2016079.pdf

National Center for Education Statistics and Bureau of Justice Statistics, "Indicators of School Crime and Safety: 2013" (2014): http://nces.ed.gov/pubs2014/2014042.pdf

New York Police Department, “Active Shooter: Recommendations and Analysis for Risk Mitigation” (2012): http://www.nypdshield.org/public/SiteFiles/documents/Activeshooter.pdf

Police Executive Research Forum, “The Police Response to Active Shooter Incidents” (2014): http://www.policeforum.org/assets/docs/Critical_Issues_Series/the police response to active shooter incidents 2014.pdf

Reiss, Dawn, “Enhancing School Access Control,” *District Administration* (November 2012): http://www.districtadministration.com/article/enhancing-school-access-control

Sandy Hook Advisory Commission, “Final Report of the Sandy Hook Advisory Commission” (2015): http://www.shac.ct.gov/SHAC_Final_Report_3-6-2015.pdf

School Safety and Security Task Force, “Massachusetts Task Force Report on School Safety and Security” (2014): http://www.mass.gov/edu/docs/eoe/school-safety-security/school-safety-report.pdf

U.S. Department of Education, “Guiding Principles: A Resource Guide for Improving School Climate and Discipline” (2014): http://www2.ed.gov/policy/gen/guid/school-discipline/guiding-principles.pdf

U.S. Department of Education, et al., “Guide for Developing High-Quality School Emergency Operations Plans” (2013): http://rems.ed.gov/docs/rems_k-12_guide_508.pdf

Department of Homeland Security (DHS): FEMA 428 - "Primer to Design Safe School Projects" (2012): http://www.dhs.gov/xlibrary/assets/st/bips07_428_schools.pdf

Contact Information

Partner Alliance for Safer Schools
www.passk12.org

Security Industry Association
8405 Colesville Road
Suite 500
Silver Spring, MD 20910
(301) 804-4700
www.securityindustry.org

National Systems Contractors Association
3950 River Ridge Drive, NE
Cedar Rapids, IA 52402
(800) 446-6722 | (319) 366-6722
www.nsca.org

SIA CYBERSECURITY ADVISORY BOARD

Beginners Guide to Product and System Hardening

The SIA Cybersecurity Advisory Board recommends a few basic safeguards to help protect security products, systems and services against failure from cyberattack. This is by no means an exhaustive list. Cybersecurity processes and technologies are constantly evolving along with the threats; the following can serve as the beginning for a larger cybersecurity plan.

These are the top 10 causes of cybersecurity failure in systems.

1. Inadequate security policy and process governance
   - Establish a department or a team that responds to reported threats.
   - Provide a way for end users and integrators to report found risks.
   - Develop a framework as to how reported threats are discovered, fixed and taken out of production.
2. Reliance on "Security through Obscurity"—assuming that nobody will ever test security
   - Assume that all of your security will be tested.
   - Use proven ports and protocols.
3. Inadequate software and firmware patching; inadequate testing of patches before installation
   - Authenticate patches; verify the update source is trusted.
   - Use patch management tools.
   - Include patches and software versioning in your change management practices.
4. Unencrypted, unauthenticated and uncontrolled wireless communications within systems
   - Proceed like the network is untrusted.
   - Remember wired is always more secure.
   - Bear in mind denial of service protection is more critical when using wireless solutions.
   - Default to HTTPS.
5. Unencrypted, unauthenticated and uncontrolled communications between systems
   - Default to HTTPS.
   - Filter IP addresses.

6. Poor password hygiene and insufficient segmentation of control system networks
   - Disable default passwords.
   - Require strong passwords before other configurations.
   - Use password-tracking tools when available.
   - Segment roles and responsibilities. (Don't use administrator privileges for non-admin duties.)
7. Lack of auditing and audit monitoring on networks
   - Periodically audit the number of network connections.
   - Periodically audit network connection lengths.
   - Use information from these audits to target anomalies.
8. Control system networks shared with other traffic
   - Ensure security networks are enterprise grade.
   - Patch regularly just as other enterprise networks are maintained.
   - Use of one network with mixed signals can be risky. When possible, segregate networks either physically or logically (VLAN).
9. Poor coding of control system software causes failures
   - Enable application whitelisting.
   - Filter out dangerous executables.
10. Lack of configuration management and tracking for hardware and software
    - Remove dormant code from firmware.
    - Track hardware and software versions when products leave the warehouse.

The SIA Cybersecurity Advisory Board's mission is to enhance SIA's cybersecurity posture and to guide the industry ahead of potential cybersecurity issues in an increasingly networked world.

Composed of several SIA Board of Directors who are cyberexperts both internal and external to the electronic physical security industry, the SIA Cybersecurity Advisory Board provides educational resources to security industry stakeholders and coordinates with other cyberforward organizations.