A White Paper

Best Practices
Concepts and Strategies

Lawrence J. Fennelly, CPOI, CSSI, CHS-III, CSSP-I
Marianna Perry, M.S., CPP, CSSP-I

Introduction:

When we editored the book The Handbook of School Safety and Security, and as we were doing our research we notice various individuals were writing 7 or 9 or 11 Best Practices and they were all one-liners. We felt at the time what was written was inadequate and lacked a high degree of updated information. So we took on the task of writing a set of Best Practices.

This set of Best Practices should be considered an ongoing project. In that if new technology comes out and its good for schools it should included. We realize that as time goes by time change and technology as well.

We had over 200 security professionals review this document and we are grateful to Michael Fagel, Ph.d. and Thomas Norman, CPP for their contributions.

Furthermore the security profession has many Concepts and Crime Prevention Strategies that can implemented to reduce crime. If you have a specific crime problem or issue feel free to contact us and we will be happy to help.

Larry Fennelly & Marianna Perry

BEST PRACTICES FOR EDUCATIONAL ENVIRONMENTS:

A Sixteen Point MASTER PLAN

Lawrence J. Fennelly, CPOI, CSSI, CHS-lll, CSSP-I & Marianna Perry, M.S., CPP, CSSP-I

This document was reviewed by members of the ASIS International Crime Prevention & Loss Prevention Council and the School & Safety Council. It was also reviewed in 2013 by fifty individuals who attended an ASIS program on School Security at the ASIS Annual Seminar in Chicago. A special thank you to Michael Fagel Ph.D., CPP and David Peterson, CPP as well, for your input.

Introduction

Master planning is a catalyst for defining a vision for security that touches all aspects of service delivery, including technology, IT integration, command and control and communication with stakeholders and employees. The plan should identify areas where security can be repositioned as a core function, contributing to the bottom line of the school. The master planning process enables security and schools to gain valuable exposure to the tools and techniques that increase the value and integrity of their campuses. Comprehensive, proactive protection solutions require collaboration among students, faculty, staff and administrators. Explore ways to adapt successful emergency response procedures to a variety of educational settings.

Part A. Administrative Procedures

1. Director of Safety and Security

- The school district or campus should have a Director of Safety, Security and Emergency Management to oversee the program.

- If utilizing a School Resource Officer (SRO) (SRO is specific to K-12, for colleges and universities, terms such as security officers, sworn officers, public safety officers, etc.) on your campus, they should be an on-duty, specifically trained law enforcement officer, who is highly visible and be required to make random rounds of the property.

- Utilize an anonymous tip line for safety and security concerns on the campus. (e.g. Crime Stoppers)

- Develop and Implement an effective Anti-Bullying Policy that is strictly enforced. (This is more for K-12 environment).

- Develop a Threat Assessment Team which includes having a mission, membership and current training by qualified professionals. It is important that the team members understand the focus and components of threat assessment and how this is different from behavior intervention teams.

- When managing your security program and software available today, anticipate the future needs of the school and campus. Install systems and programs with long-term expansion capabilities to accommodate for future security needs and upgrades.

- Be aware that electronics and technology alone do not make a "Security System." They are just one of the tools in your toolbox and you have to put the right mix of technology and people in place to work in conjunction with the other components in your overall security system.

- To provide your school or organization with the best IT security possible requires a mixture of both enforcement and education. Employees have more freedom than ever before and that means they need to take more responsibility for their own safety than they may have done in the past. You can eliminate opportunities for risky on-line behavior by having the appropriate policies in place so you don't waste valuable time reacting to problems and can spend more time anticipating vulnerabilities in your IT system. You must be proactive and take practical steps to protect your school or organization <u>before</u> there is an issue.

2. Vulnerability Assessment

- Our culture has changed and crimes against students and staff on school property have changed, as well. Needs and deficiencies must be determined in order to have a security program that is effective.

- A Vulnerability Assessment is a critical (well thought out) on-site examination that is used to observe security that is currently in place, identify security deficiencies or excesses, determine what level of security is needed and finally, to suggest options for consideration to assist in the mitigation of identified areas for improvement that may assist in lowering the overall risk profile. If implemented, these recommendations will effectively control the identified risks.

- After the Vulnerability Assessment, you and the assessor together will conduct a cost/benefit analysis to determine what the prioritization should be for the presented findings and options for considerations and implementation, while being cognizant of budgetary and other factors that may affect timelines and implementation. It will be determined if the recommendations are affordable, feasible and practical. They will be budgeted as short-term or long-term projects.

- The assessor will utilize and gather statistical data from law enforcement, such as, UCR, NIBRS, NCVS and DHS to examine the frequency and severity of events in your area to determine what can be done to remove or reduce the threat to your campus.

- A Vulnerability Assessment should be completed annually (or more often if there are issues or significant changes to the building or campus environment) by a qualified individual. At this time, a review of all programs, policies and training will be done to ensure that you are addressing current security issues.

3. Security Program Management

- Establish security policies and procedures that address identified risks and ensure that the security program has the approval and "buy in" of the school district and principal of the school for K-12 and administration for colleges and universities. It is important that policies and procedures are documented and address Violence Prevention and Intervention and are supported by school faculty and staff or administration. Consistent training and enforcement are essential.

- The school district as well as each individual campus, need to effectively manage their security program using multi-levels of communication, polices

and procedures, physical security, training, as well as response plans. There should be an effective process for short-term and long-term projects.

- In K-12, involve the parents (PTA and other volunteers) and students in your school safety/security program to assist and help educate students about policies and procedures.
- In both K-12 and college/university environments, form partnerships and strive to involve the community (law enforcement, businesses, homeowners, property owners, houses of worship, civic groups, etc.) to help keep your campus safe.
- Identify and manage your assets by ensuring all prevention, detection and notification systems (alarms, lighting, video surveillance, intercoms, mass notification systems, etc.) are working properly and that high-theft and high-risk areas have the proper coverage.
- Integrate solutions with existing security systems and infrastructure for maximum return on your investment.
- Lock classroom doors while class is in session with properly installed and effectively maintained hardware.
- Educate students, faculty and staff about the function of the Threat Assessment Team and how to report situations of concerns.
- Educate students, faculty and staff about bullying behavior. (harassment/mobbing, etc.)
- Inform students, faculty and staff that they should report and/or challenge anyone on the property that is not displaying an ID badge. This doesn't work for all settings.
- Educate students, faculty and staff about "If You See Something, Say Something" and empower them to report suspicious behavior or behaviors of concern.
- Educate and train staff in all school security policies and procedures and repeat training as needed or when a change is made. Faculty and staff must consistently follow and fairly enforce all security procedures. There must be clear disciplinary action for anyone not following established rules or procedures.

4. Background Checks

- Conduct comprehensive (as the law allows) background investigations (pre-employment, annually or as-needed/for cause) and drug testing for all faculty, staff, volunteers, contractors and vendors who are on school property. Some of this will apply to K-12 only.

- For K-12, implement fingerprinting program for ALL school faculty, staff, volunteers, contractors and vendors who are on school property.

Part B. Physical Security

5. Lobby of the Administration Building this entire section is specific to K-12

- Install an intercom with appropriate digital video verification and door release button, inside the lobby vestibule or in the administrative offices.

- Have Digital Security Surveillance System (CCTV) monitoring the area.

- Issue and require all students (in grades 9 to 12), faculty and staff to visibly display color-coded, ID badges (or smart cards). The size and orientation should be changed yearly, with vertical for staff and horizontal for students with color bars or color background to clearly identify students from faculty and staff.

- Implement an effective and easy to manage Visitor Management Software System, including sign-in, photo verification, badge issue and escort, if required. Use a driver license scanner for positive visitor identification. Consider a color-coded badge system for access to specific floors or areas.

- Utilize a computer database sign-in either in the lobby or on-line when appointments are requested.

- Exterior doors should be locked at the start of school day (others are egress only and monitored) and only one entrance should be utilized that is equipped with intercom and Digital Video Surveillance System.

- Determine if walk-through metal detectors (magnetometers) and/or hand held scanners need to be utilized.

- Utilize a panic button/duress alarm in the lobby, which transmits a signal to a central station who in turn will notify law enforcement, if there is an emergency situation.

- Have a written and practical procedure for the use of panic/duress alarms. Determine if this should include an automatic lockdown of the school.

6. Signage

- Install signage on the campus to direct visitors, contractors and vendors to the office area to be processed for access.
- Post Gun Free Zone signage as a first line of defense against Active Shooter situations.
- Doors (interior and exterior) and windows need to be identified by placement of a number or letter (which is approved by Police and Fire/EMS responders) to identify various rooms in the building and on the campus. Obtain information from other schools and your local fire department to meet standards. Some schools currently have 10" to 12" high room numbers. Use the same size numbers on front door. (Consider using retro-reflective, 3M Scotch light type material).
- In conspicuous locations, post emergency escape route of travel maps on walls in all buildings and in all rooms.
- Utilize luminescent marking at floor level for crawling in smoke to help mark EXIT routes.

7. Perimeter of the Campus

- Clearly identify the perimeter of the campus and utilize the CPTED concept of territorial reinforcement so school property is easily identifiable from public property. Install fencing and appropriate lighting, as necessary.
- In remote or high risk areas of the campus, consider the ASIS International standard for fencing: 7' in height (with 3 strands of barbed wire if necessary), placed 6 inches apart.
- Follow the CPTED Concept of maintaining bushes no higher than 3 feet and tree branches trimmed to 8 feet from the ground.

8. Perimeter of the Building

- Improve/upgrade/maintain the door hardware on all outside entry doors and install anti-prop alarms.
- Install strike plate security devices to prevent shimming or prying of the door.
- Have full perimeter lockdown capability—either manually or automatic, but ensure that it meets local codes.

- Consider the use of effective bollards to prevent vehicular access to buildings.
- Enforce the policy of no parking areas and designated drop-off areas. No standing/no loitering areas must be addressed and enforced.
- Before planting shrubs or bushes around buildings, consider the growth rate and the maintenance that will be required. Bushes should be no taller than 3 feet and set back 1 yard from buildings or walkways, per CPTED concepts.

9. Access Control Systems

- An electronic access control and audit database with an anti-pass-back feature should be utilized.
- Keep access points to a minimum. The general idea is to have one (or few) entrance(s) and many exits.
- Monitor the school parking lot with video surveillance and issue color-coded parking permits with designated parking areas for students, faculty, staff and visitors.
- Before an incident occurs, ensure first responders will have access to buildings (issue all-access cards or master keys at training exercises).
- Install KNOX or SUPRA type key boxes as required by the local authorities having jurisdiction. Contents should include floor maps, access cards, keys, photo binder, location and layout of high-risk or specialty areas and the location of special needs refuge areas. Do not rely on video surveillance as your intelligence tools. Maps and photo binders are critical in technology failure situations.

10. Key Control

- If you do not have 100 % control over your master and grand master keys, then you must re-key.
- Do not issue grand or grand master keys to staff. Adequate key controls must be in place.
- Establish a Key/Card Management Program and assign someone to manage it.
- Re-key mechanical locks if keys are lost, stolen, not returned at a termination or of keys are otherwise unaccounted for.

- Consider the use of keyless access control systems so that access can immediately be terminated if a card or code is lost, stolen or if someone is terminated.

11. Lighting

- Install adequate lighting on campus—especially by walkways, around doorways and in parking areas. A properly illuminated area acts as a psychological and physical deterrent and can reduce criminal opportunity.
- Refer to OSHA, IESNA and ANSI for lux and foot candle lighting level recommendations. Test illumination annually with a light meter and be cognizant that foliage on trees may obstruct lighting.
- Be aware of light trespass on neighboring properties.
- Consider installing cost-effective LED lighting for ROI.
- Have a Lighting Maintenance Plan in place to quickly identify burned out bulbs or inoperable lights. Assign and display numbers on light poles so those requiring attention can be easily identified. Inoperable fixtures or burned out bulbs must be repaired or replaced within 24-hours.
- Lighting needs to be uniform and cost effective, with the proper illumination levels.

12. Digital Video Surveillance

- There should be wide deployment of Centralized Digital Video Systems, managed by Video Management Software.
- Retain at least 30-days of recorded surveillance, unless otherwise required.
- Utilize digital recorders and consider cloud-based storage.
- Ensure video surveillance coverage is adequate and utilize effective and accessible video analytics.
- New analytics can detect a threat and then broadcast an alert to inform the community where the threat is and where to go to avoid it.
- Audio analytics are now being used to detect gunfire and send an alert to a computer, i-pad or smart phone.

- Install IP HD video cameras and determine if you need a fixed camera or a pan, tilt, zoom (PTZ) unit. (PTZ cameras work well, but are expensive)—almost 3x cost of a fixed camera and need on-site monitoring to be effective. Budget for this type of investment. Determine the purpose of you video surveillance program, monitoring and response, forensic purposes only, or both.

- Design the system to allow remote viewing using an i-pad or smart phone when not on the school property.

- Exterior lighting should be adequate for video surveillance resolution and color rendition index (CRI).

- Integrate video surveillance with access control, especially visitor management.

- Install video surveillance around the perimeter of the buildings, with attention to doors and accessible windows.

- There are standard locations established for certain types of cameras and monitoring. For example, at the main entrance, exterior entry points, cafeteria, hallways, high-risk areas, high theft areas, computer labs, etc. Cameras are <u>never</u> installed at any location where there is a reasonable expectation of privacy, such as in a restroom or a locker room. Cameras are also typically not put in instructional areas such as classrooms. There may be other areas identified by school staff, faculty or assessment that are identified as “hot spots” where video surveillance would be beneficial.

- Cameras mounted near main entrances and in administrative offices can help you record each visitor as they enter and exit. Cameras near exits can help reduce truancy.

- Use fixed cameras strategically placed to protect valuables such as computers, sound and video equipment, trophies, library, etc.

- Outdoor surveillance cameras monitoring the school can prevent vandalism. In parking lots video surveillance can help protect students and staff when leaving late or arriving early.

- Integrate video surveillance with alarm (intrusion detection) systems. For example, if a door is propped open, the camera zooms in to determine the cause and then sends notification that a response is required.

- Establish a partnership with local law enforcement and give them secondary monitoring capabilities of the centralized video security system for coordination of first responders to a critical incident or crime in progress. If the school has an intrusion detection system and it is activated at night, law enforcement or security can respond remotely and disrupt a crime in progress. In this instance, video surveillance may also be used as evidence for prosecution.

- Back up video surveillance (that may fail immediately) with still image mapping or a 360 degree photo inventory similar to what realtors use when showing property. This photo image may be the only reference point available to responders if the hallways are smoke filled or the video surveillance is looped or de-commissioned.

- Install cameras in vandal-proof domes. This is essential in a school setting where there is a constant flow of students who may vandalize or attempt to disable the camera.

13. Fire Alarm Systems

- Conduct regular fire drills to ensure faculty and staff can quickly determine if all students are accounted for. Your Visitor Management System will help you determine if all visitors have been evacuated in the event of a fire or other emergency.

- Comply with all applicable state and local codes

14. Emergency Planning

- Develop an effective and comprehensive, Emergency Response Plan. Provide training and education for the faculty and staff.

- Comply with **all** applicable state and local codes

- Establish Emergency Procedures with standardized actions and directives for inclement weather, (tornado, earthquake, hurricane, flooding, etc.) medical issues, fire, building evacuations, shelter-in-place, lock-down, workplace violence, active shooter as well as a business continuity plan for after the incident. (OSHA, NFPA, FEMA, etc.)

- Ensure your Emergency Procedures comply with ADA Standards (physically handicapped, visually impaired, hearing impaired, special needs students, faculty, staff and visitors, etc.). Have designated individuals trained to assist.

- Conduct regular training and joint exercises for emergency procedures with the local FD, PD, EMS and other local officials. Provide floor plans for each building on the campus to each of these departments. Consider supplying building plans and layout of campus in a digital format on thumb drives for quicker access by more responders. Update the thumb drives that can be issued to teams on a quarterly basis. The main servers may be down, as well as cloud-based, so a thumb drive for a laptop may be the only available tool. (Install thumb drives in exterior locked Knox or Supra Boxes)

- Establish a Crisis Management Team with documentation, training and integration into the larger Incident Command Team.

- Determine who has the immediate authority to lock down, issue CLERY alert for higher education and talk to the press. Establish a Joint Information Center with appropriately trained public information officer that can supply vetted information that comes from the command staff only.

- The Crisis Management Team will integrate into the response and recovery operations and will work closely with the first responder community as the situation ebbs and flows.

- Develop procedures for during and after a crisis situation.

- Develop Mass Notification Procedures (see below).

- Provide two-way radios batteries, chargers, cases and training (or another alternative method for communication) for faculty and staff and establish a designated command center area or location.

- The staff should follow the prescribed plan and report to the Emergency Command Center, (ECC) or other pre-designated area for response and recovery. This may not be at the same site due to safety reasons and may be at a remote location.

- Administrators will need to be at different locations and not in the immediate area of the event for their own and response operations safety.

- Ensure you are in compliance with all applicable OSHA regulations, Life Safety Codes and local/state fire codes.

- NFPA 1600 is a useful tool to help comply with for all risks and all-hazards planning.

- Provide FEMA training for administration and crisis team members.

http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-100.sca.

- Conduct fire, evacuation, lockdown, shelter-in-place, etc. drills.
- Consider using the standard response protocol," I love u guys foundation."
- Develop crisis kits with all necessary supplies for an emergency situation.
- Develop GO BAGS for action teams.
- Establish markings, vests, hats, or other readily identification so that the school teams can be effectively identified to appropriate response officials.
- Develop an effective and practiced mutual aid agreement with other schools and businesses.
- Collaborate with local law enforcement and all emergency response officials to establish protocols for shades and green cards to determine if interior door windows are to be covered and/or if shades are to be left open or pulled down in a lockdown situation.

15. Mass Notification Procedures

- Develop a Mass Notification Program, which includes e-mails, text messages, social media, public address system announcements as well as audible alarms.
- This must use pre-scripted messages and messaging must be approved by the Incident Command Staff (not a committee) before being broadcast.
- Ensure your Mass Notification Program complies with ADA Standards (physically handicapped, visually impaired, hearing impaired, or special needs students, faculty, staff and visitors, etc.). Have designated individuals trained to assist. Provide language assistance and pre-established phone trees.
- Ensure that your procedures meet NFPA Standards & Guidelines, which includes a communication program, an incident management system and with individuals that can effectively understand ICS and the procedures and protocols. There must be at least three people trained per-position in the Emergency Management Organization.

16. Training for Faculty and Staff

- When hired, conduct classroom training on school policies and procedures. Repeat annually at in-service training or as necessary.

- Schedule annual mini-exercises (not for failure but for reinforcement).
- Schedule regular active shooter reaction training.
- Develop a policy for faculty and staff about when to use a fire extinguisher. OSHA Regulations state that if a person is REQUIRED to use a extinguisher as part of his/her duties, they must be adequately trained in fire extinguisher operation and selection. If fire extinguisher use is voluntary and not required, then the training obligation is diminished.
- Always insist that upon discovery of any fire, regardless of the size, to notify the Fire Department and sound the appropriate alarm.
- Discuss when to fight a fire or when to flee a fire. Train staff on how to use a fire extinguisher. Adequately train per OSHA and state regulations.
- Conduct First Aid, CPR/AED and Bloodborne Pathogens Training (29 CFR 1910. 151) and repeat re-certification as required. Understand whether or not giving first aid is a requirement vs. voluntary, as this involves Heptavac Vaccine, training, personal protective equipment and appropriate universal precautions.
- Conduct training on how to respond to medical issues, fire, inclement weather, building evacuations, shelter-in-place, lock-down, workplace violence, active shooter, etc. Appropriately trained staff will educate students as to the appropriate policies.
- Ask local, state and federal agencies to participate in your classroom, tabletop or incident training.