From natural disasters to foreign or domestic terrorism, the United States faces formidable safety concerns. Does your campus have an emergency plan?

PROTECTING THE CAMPUS:

Don't Forget to Plan for Your Plan.

Jason Wolff, WESCO Senior Application Engineer

WESCO®

OMNIA PARTNERS

When it comes to providing a safe, healthy, and constructive learning environment for our youth, it is imperative that we think beyond traditional security measures. We are all aware that, due to the rising price of precious metals, we face critical asset vulnerabilities — from the simple theft of copper buried near a building to that of gold from a vehicle's catalytic converter. The loss of such assets clearly has a monetary impact. But that pales in comparison to protecting our country's most critical assets — students on educational campuses across the nation.

Protecting our youth and understanding vulnerabilities often requires additional thought and more discussions than does traditional planning for protecting a transportation corridor or courthouse. We must strike a delicate balance between providing a free, open campus and safeguarding students. As such, campus security requires considerable ingenuity, coupled with a strong understanding of how to leverage legacy security assets with more modern, efficient systems.

Physically securing places where people gather in large numbers should be a top priority for anyone responsible for school and campus security. Where to begin? The first step is to plan for your plan, and we have provided guidelines below to help you implement a planning team who will ultimately be responsible for developing an Emergency Operations Plan (EOP) to protect your campus.

INITIATING THE PLANNING TEAM AND EOP

Effective campus protection begins with establishing an emergency planning team and charter. A dedicated crew with top leadership support from a motivated sponsor, such as a University President, School Board President, and/or Superintendent, is of enormous value, as these folks lend credibility and authority when the time comes to implement the plan across the campus population.

At the federal level, the Presidential Policy Directive (PPD) 8 defines planning and preparation for all critical assets, including educational institutions. First responders, risk assessment professionals, and school officials should be well versed in PPD 8, and in implementing best practices across five mission areas: Prevention, Protection, Mitigation, Response, and Recovery.

Once the emergency planning board's charter is approved, we recommend following the fundamental planning steps outlined below in order to create your Emergency Standard Operating Procedures (ESOP) or Emergency Operations Plan (EOP). These steps will not necessarily fall in sequential order and may well overlap depending on your campus' specific needs.

1. Conduct a Risk Assessment and Vulnerability Plan (RAVP)

This can be accomplished before the Planning Committee is completely assembled. Consider inviting a third-party security professional to conduct a site survey of your campus and critical areas, because an objective opinion that is free from bias and preconceptions can be very helpful. The resulting report can help the Emergency Committee identify weaknesses around campus,

like bottlenecked emergency exits, large student gathering areas, unprotected critical infrastructure, such as power stations, network operations centers, or communication closets, and security booths and laboratories. The report should also assess avenues of approach and escape for any person committing mayhem on the campus. The RAVP can be extremely detailed and thorough, identifying countless areas of risk and hazards for the committee to review.

2. Nominate Committee Leadership.

Early in the process, the Planning Committee sponsors will nominate a leader to build the team. The following personnel are recommended to be on the Planning Committee:

- Supervisory person (Dean, Vice, Head of Security, etc.)
- Student body representatives
- Instructor representatives
- Custodial representative
- Local first responder, if available (police, fire, EMT)
- Other employee representatives on campus

Reach out to federal, regional, state, county, and local FEMA or Emergency Management personnel and request representation at your planning and training.

Don't forget that privacy issues need to be considered. It is imperative that your legal team review the Family Educational Rights and Privacy Act (FERPA) prior to allowing any access to student records for behavior or predictive analysis during any of your planning. Non-campus employees who are members of your Planning Team must meet FERPA criteria if they are to become eligible to view such information.

Once a team is assembled, it is time to brainstorm all conceivable or possible threats to campus. The RAVP team can assist the Planning Committee with this if needed. Earthquake, a swarm of killer bees, or an active shooter situation...every scenario needs to be considered and weighed, regardless of mitigation or budget. The Planning Committee will then determine which threats are truly applicable.

3. Begin the RAVP analysis and build the Emergency Operating Plan (EOP).

Once all potential threats have been identified, the physical structure and layout of the campus needs to be considered. A full scale map, model, or drawing of the campus should be constantly displayed and referred to. This "campus picture" provides a visual representation of an event as it would unfold, and helps the committee develop a plan for how the campus Emergency Response Team and First Responders should react to most effectively mitigate each threat.

In a scenario where a pipe bomb is detonated in the stadium during a football game, for example, studying a campus map would provide a bird's-eye view of how people might scatter/run/hide, and how First Responders could enter the facility. After simulating such an event visually, response tactics can later be practiced during actual training exercises.

During this step, details of Standard Operating Procedures (SOP) should also be discussed. This includes not only identifying the best reaction plan to an event, but also formulating ways to prevent the event from ever occurring in the first place. Because it is impossible to identify or predict every possible threat, especially during a terrorism event, it is critical that the planning committee leadership has solid, experienced security professionals on staff.

4. Establish an Emergency Operations Center (EOC).

At this time, an Emergency Operations Center should be designated or planned for on campus. The EOC must be secure and have robust communication capabilities. Networks should be both wired and wireless, and a Radio Frequency (RF) net control area should be set up to allow two-way communications should the phone (VoIP or POTS) network become unavailable. Back-up emergency power is necessary, as well as dedicated HVAC and air ventilation. The main focus of the EOC is to enable communication with organic security assets on campus and First Responders off campus.

In addition, the EOC should have direct access to the mass notification system (if one doesn't exist, it is highly recommended) and all security cameras and sensors. The EOC should be in a hardened, brick-and-mortar facility able to function (communicate) on its own power supply for a designated period of time.

Ideally, the campus should also have an established Alternate Emergency Operations Center (AEOC). Depending upon threat and risk assessment, the AEOC should not be co-located with the EOC, and should not share any power or network feeds the EOC utilizes, with physically separate pathways and with no cables that "pass through" the other's cables on their travels back to the power source or network closet.

Finally, it is important to note that cell phones should never be depended upon as a primary means of communication in an

emergency event. Communication management is like air for any ESOP. No matter how well the EOC is operating, the response to an emergency event requires clear, concise, and accurate information being shared from the security managers to the outside world.

5. Test and update your EOP.

Your EOP should be flexible and reviewed periodically. In addition to a periodic review, lessons learned from campus emergency exercises, peer reviews from other campuses, or real world events should be studied and considered on a consistent basis. You should also consider any new campus technologies, buildings, roads, or structures, which may result in the need to revisit and adjust your plan. The bottom line is that your EOP should evolve as necessary, and adjusting your EOP should not be a difficult process. Revising your EOP should be a collaborative effort and include feedback from the entire Emergency Committee.

FOCUSING ON PROCESS

The planning team or committee's progress should flow through a controlled step-by-step process. This process, specifically RAVP analysis and mitigation planning, begins with the formation of the team mentioned above. A key step in planning is to prioritize the identified risks using an approved scale and to establish the allocation of resources to mitigate these risks. Qualitative and quantitative risk assessments are outside the scope of this whitepaper, but utilizing both of these methodologies could be extremely effective in this process. Another key element is to always establish and maintain clear lines of communication with your Executive Sponsors throughout each step of the process. As previously mentioned, these sponsors will be critical allies when it comes time to conduct training exercises for events, such as an active shooter or large earthquake drill. The more disruptive (large) the exercise, the more assistance and approvals you will need from your Executive Sponsors. Keep them informed and always know who your champions are at the executive levels.

When developing an EOP, there are three critical, questions to ask:

1) What are we going to mitigate?
2) Where shall we place our limited resources?
3) What solutions are available that we might consider?

Unsure what solutions are out there? Then do your research! Your planning and security teams should visit security trade shows, invite security integrators to campus to educate leadership on the latest technologies, and conduct their own due diligence, both on the internet and by reading trade magazines. And remember, new technology does not necessarily mean larger budgets, so look at every option. Saturating a dormitory or sensitive science lab with expensive security cameras may not be the best value or most secure solution for your specific campus. Did you know that tying in a modern, inexpensive Intrusion Detection System to detect initial movement can significantly reduce the need for HD Cameras by over 75%? Study your options and educate your Executive Sponsors about the different technology options you're considering before you submit a formal funding request.

One technology that's becoming more prevalent across campuses is an Active Shooter Detection System. Properly surveyed, designed, and installed, it can provide instantaneous location and time for any gunshot on or near the campus. This warning system works both inside a building and outside, and ties into the existing Public Address or Mass Notification System. With simple management software, a system can simultaneously send instant alerts via SMS, email, basic flashing alert lights, and/or phone calls to select individuals on and off campus.

APPROVAL

Once the plan is written and approved by the committee, do not delay in getting Executive Sponsorship feedback and approval. Ensure that all key personnel outside the committee understand the goals and purpose of the plan, and that the required stakeholders are trained on what they need to know. Cross-training your stakeholders on job duties is strongly recommended, because it reduces single points of failure that can occur when personnel have sole possession of institutional knowledge.

TRAINING EXERCISES

Once your plan has been approved, but prior to implementing the schedule for planned exercises, conduct carefully coordinated and periodic Emergency Planning Meetings (EPRs) to ensure all stakeholders are aware of each training exercise and all that it entails. Communication and discussions between campus officials, safety officers, and their peers on other campuses can have an enormous impact on the success (or failure) of these exercises, as well as on your overall safety objectives. Make sure that everyone involved knows their places, roles, and responsibilities.

For example, students should understand where lockdown shelters or rally points are. The instructor should know where the EOC and AEOC are located, and how to communicate with them. Use the exercises as not only training, but also as an upfront hands-on review of the SOP to determine what immediate adjustments might be needed. An example of this might be discovering that your Alert Software has yet to be programmed with your First Responder's contact information. Training exercises are the ideal time and place to identify and address such issues.

Post exercise, conduct an After Action Review to help minimize the risk of operational issues (which can result in a phenomena known as the "Haze of Panic") in the event of an actual emergency situation. History has taught us that during actual security events, organic intelligence cannot and should not be the primary source of information used by First Responders and campus security personnel. Key personnel require real-time, accurate situational awareness information to make timely decisions, shelter in place, run to specified rally points, or in the worst case scenario, fight back. So do your best to identify and mitigate these risks (reduce the "Haze") during the planning stages of building your Response Strategy. Your goal should be to always incorporate lessons learned into your SOPs and EOPs.

OUTPUTS FROM THE PLANNING COMMITTEE

There are several parts to the actual EOP, including the annex portion which spotlights Courses of Action and how to implement them. As mentioned earlier, it is almost impossible to identify, assess and mitigate all risks, but that should never deter the team from developing these functional annexes.

Please keep in mind that the information presented in this whitepaper is simply the tip of the iceberg. Entire chapters could be dedicated to each and every point covered.The guidelines we've presented are in some cases mandated by federal, state, or local laws, and in other cases they're simply best practices developed to help ensure that we are all doing everything we can to protect the children, faculty, and visitors at every campus across the nation.

WESCO's dedicated technical team is ready to work with your campus to implement a real plan to prepare you for any threat.

LEGAL DISCLAIMER: This discussion is an exercise examining a complex issue. WESCO is not advocating a specific EOP; rather, each organization should consult internally with management and externally with outside experts in light of their specific unique situation to develop an effective EOP.