Guidepost

SECURITY PLANNING DOESN'T HAVE TO SINK YOUR BUDGET

We were recently asked by an architectural firm "…how can we implement security features for active assailant scenarios into our designs?" This was quite refreshing, as the typical request for active assailant assistance is to conduct on-site scenario-based training. While training is important, it can be ineffective unless followed by regular practice, i.e. developing "muscle memory." And, it is but one tool in the box of prevention and response options. There are many additional proactive measures that can be taken to prevent or minimize the probability and impact of an active assailant incident. Some of these are physical and psychological, others operational, and yet others electronic in nature. Below is our response to our architectural colleague.

Crime Prevention Through Environmental Design

Without question, Crime Prevention Through Environmental Design (CPTED) elements should be considered as a part of architectural design, especially in the area of creating natural visibility and sightlines throughout the interior of a facility. Exterior visibility and sightlines should also be maximized through lighting and landscaping. The topic of sightlines cannot be overstated. Elements such as panoramic stairwell facades, and "eyes on the street" concepts are well established and effective. While natural access control and territorial reinforcement do not have a significant impact on the active assailant scenario, they can minimize it a bit, and counter other criminal vulnerabilities. Finally, target hardening is unrealistic when looking at an entire facility, but certain critical internal areas might justify protection against active assailant threats. Progressive collapse prevention should be considered for critical areas as well.

Designing open office space that allows for freedom of movement in multiple directions at all times can facilitate quick escapes away from threats and toward safety. Creating areas of refuge using existing forms, such as bathrooms, should also be considered. In addition, elements such as color selections, and maintenance of a site, can have a psychological impact on site ownership (for both undesirables and occupants).

Designing for vehicular protection typically takes the form of aesthetically unattractive measures such as bollards, when in fact, the same can be achieved through well thought out barriers such as berms, seating walls, artwork,

landscaping, water features, etc.; at a lesser cost than bollards or equivalent. Further, vehicular velocity (i.e. penetration impact) can be reduced through traffic circles, circuitous routing, speed bumps, etc., thus reducing the strength requirements (i.e. costs) of vehicular barriers.

Operational Options

Proactive operational measures should start with ensuring proper employee and contractor vetting, as well as active social media monitoring for threats. Ensuring that all employees are trained to recognize and report signs of workplace violence is also a must and should include the use of employee hotlines, and teams (HR and Compliance) well-trained on managing reports of this nature. In addition, employees should undergo general security awareness training that can be applied at work, while travelling, as well as in their personal lives.

Other operational considerations include ensuring the structure of a crisis management team that includes clearly defined roles, responsibilities, and communications between members. Further, active assailant type scenarios should be "table topped" on occasion.

Lastly, the contentious topic of arming on-site security personnel should be discussed. The reality is that most active assailant incidents are resolved only upon the arrival of armed responders. As such, the theory of having armed responders already on-site implies a quicker resolution to such an incident.

Electronic Options

Electronic countermeasures should focus on "building lockdown" infrastructure. Building lockdown is primarily a sequence of electronic actions and interfaces that are immediately, and ideally automatically, initiated when an active assailant threat is recognized, and includes some or all of the following considerations:

- Automatic and immediate notification to emergency responders
- Alerting internal security teams and control rooms, both local and remote
- Activating site/building perimeter access control for card reader use
- Deactivating interior access controls to allow for free unhindered movement
- Opening lobby or delivery area controls, again, allowing for free unhindered movement from these public spaces
- Recalling vertical transport (elevators) to upper floors
- Disabling ground floor fire "pull" stations (if allowable by local authority)
- Initiating building wide annunciation of the event (only where training has taken place)
- Incorporating audio ("gunshot") and video ("weapon") analytics for early and automated detection

Active assailant preparedness has gained significant attention given the increase in the number of such events over the past decade. While the above are considerations for this type of threat, these controls also combat other threats such as crime, terrorism, workplace violence, natural disaster, and fraud, and they comply with the overall duty-of-care all organizations are required, or should be required, to provide. Equally important, you should note that most of these controls also represent existing spend, i.e. things that you are already doing, and that if approached from a security standpoint, can achieve far more than originally planned. Security planning won't sink your budget if you proactively

align it with your design and infrastructure plans.