ASIS International Cultural Properties Council

Target Hardening Suggestions

Short Term (Right Now!)

- Remember your organization's mission and ensure you continue to follow it
- Raise awareness by communicating with your staff.
- Learn and understand your staff's concerns.
- Discuss with local law enforcement potential threats to your institution.
- Let staff know how they can help, e.g. "If you see something, say something."
- Know what your neighbors are doing. Sharing ideas and information helps build a resilient community.

Long-term

Site Survey and Risk Assessment (Annual review at minimum):

- Look at your institution with a fresh pair of eyes to uncover potential vulnerabilities.
- Review your policies and procedures.
- Review all the resources at your disposal, both internal and external
- Learn and understand ongoing concerns of your staff.
- Discuss with local law enforcement potential threats to your institution.
- Review your institution's daily operating procedures to understand how any changes in security procedures might adversely impact them.

Plan and Implement Solutions

- Develop a plan of action based upon your site survey and risk assessment.
- Physical site hardening takes time, planning, and money, all of which might not be possible, nor a cost-effective means of addressing your institution's risks.
    - Do ensure that what physical security measures you have are working and in good condition—locks, doors, gates, bollards, access control, fencing, CCTV
- Communicate your plan
    - **Internal:** emails, staff newsletter, staff meetings, training manuals and training sessions
    - **External:** let local law enforcement know your concerns and see how they might be able to assist you with an increased presence at your facility
    - **Make sure all your internal and external contact information is correct and up to date.**
- Implement a heightened alert plan when threat levels increase. A pre-determined plan with action items that can quickly be implemented in order to raise organization wide security awareness and response to counter and reduce the threat.
- Move security posts to forward positions and provide security officers with specific post orders designed to counter/ reduce the threat.

- Perform staff training
    - Review policies and procedures with your staff on what to do in various emergency scenarios—***make it real for them!***
    - Tabletop exercises and drills will help reinforce training
    - Let all staff know that they can help through their own observations
        - If you see something, say something
        - Trust your instincts and report any suspicious persons, suspicious behavior, and suspicious packages

- Consider a behavioral approach to target hardening
    - The Mall of America uses trained plain clothes security professionals to engage visitors whose activities are out of the norm.
    - All potential wrongdoers fear detection and so will display certain typical stress characteristics
    - Create a baseline of what is considered "normal" behavior at your facility. Activity out of the norm might be a single male in his 30s spending time in an area where the average visitor is between 5-10 years of age accompanied by one or two parents. This approach allowed one of security officers to identify a vagrant who was eventually removed from our grounds.
    - Define what suspicious behavior is specific to your organization and train all staff (security and non-security staff) on how to report or respond when suspicious behavior is observed. What is suspicious in one organization may be normal behavior in others. For example taking photographs and video at a museum is normal guest behavior but it is not normal for photographs or video be taken of security equipment, posts, employee areas etc.
    - Engage every visitor to your institution with a simple greeting. The retail industry has deployed this security tactic effectively for years and studies have shown that such an approach does reduce criminal activity.
    - If you have the resources, consider having some of your security officers work in plain clothes in order to help detect any possible perpetrators, such as pickpockets during times of high visitation

- Screening
    - All deliveries to your facility
    - If you have the resources, consider screening all visitor vehicles and bags
    - Consider a package or bag policy that will not allow visitors to enter your facility with any package or bag beyond a certain size. Best of all possible worlds is a no bag policy, but this might be practical for the visitors to your institution based upon your culture and risk profile.

Employee Travel

- Review the US Department of State website for updated travel warnings and alerts.
- Staff traveling on company business should provide detailed itineraries so their locations can be pin-pointed if and when something happens. Whenever a terrorist event occurs somewhere in the world, one of the first questions your organization should ask is: "Do we have any staff traveling there?"
- Those who work for a company that travels abroad you can sign up for the OSAC report and receive daily which is always informative for specific countries or this sort of alert.
- Advise your staff that they should register with the local US consulate abroad, if there is one, and you should have a planned exit strategy, such as first flight out of a war zone to first safe destination.

Key Points for Security Personnel

1. Be visible
2. Be vigilant
3. Be proactive
4. Engage all visitors and staff
5. If you see something, say something