ALLIED UNIVERSAL®
There for you.

Active Assailant Preparedness Resource Guide

INTRODUCTION

Active Assailant incidents have become a pervasive and frequent threat in the United States over the past 20 years. These frightening and seemingly random incidents have impacted countless organizations across the country—from school campuses and retail centers to office buildings and hospitals. The message is clear: no matter your industry or geographic location, your organization needs to prepare for the possibility of violence.

Your organization's security program is simply incomplete if it does not include a detailed plan with key tactics to address the Active Assailant threat. At Allied Universal®, we have developed a robust and comprehensive Active Assailant Preparedness Model to help our clients identify the relevant security solutions and services that can help them mitigate threats and reduce vulnerabilities at their facility, all with the goal of preventing an Active Assailant incident before it even occurs.

Our Preparedness Model is inspired by key findings and recommendations from the field of Active Assailant research. Specifically, our model aligns the phases of the "Pathway to Violence" and the "Eight Critical Factors," described below. Combining these two models allows Allied Universal to move academic research from the realm of theory to the practical and to show our clients when and how security tactics can be implemented to impact the likelihood of active assaults.

PATHWAY TO VIOLENCE

Although Active Assailant incidents may seem sudden and unplanned, research shows there is a typical multi-step Pathway to Violence commonly followed by most assailants. Understanding this pathway is the key to successfully intervening at each step with relevant security tactics.

1. Pre-Threat
2. Threat Actor Grievance
3. Violent Ideation
4. Research & Preparation
5. Arrival at Site
6. Commits Assault Act
7. Retreat/Neutralization

EIGHT CRITICAL FACTORS

The Eight Critical Factors listed below are modelled on key safety tactics recommended by the Department of Justice. Addressing these Critical Factors can help mitigate the risk of Active Assailant violence and facilitate swift and effective law enforcement assistance.

- Comprehensive Threat & Vulnerability Assessment
- Organization Climate & Culture
- Building & Environmental Safety
- Anonymous Reporting System
- Public & Private Partnerships
- Behavior Threat Assessment & Management
- Mental Health Resources
- Training, Exercises & Drills

Source: Office of Community Oriented Policing Services, Department of Justice. 2020.

PREPAREDNESS MODEL

To help improve safety and reduce vulnerability, Allied Universal® recommends implementing key security solutions for incident preparation and response.

1 PRE-THREAT

- Threat/Vulnerability Assessment
- Virtual Threat Assessment
- Threat Management Team/Program Creation
- Workplace Violence Policy & Procedure Review/Creation
- Workplace Violence Awareness/Prevention Campaign Creation
- Anonymous Reporting Hotline
- Emergency Response Plan Creation
- Emergency Response Plan Training & Exercises

2 THREAT ACTOR GRIEVANCE

- Threat Management Team/Program Creation
- Workplace Violence Awareness/Prevention Campaign Creation
- Anonymous Reporting Hotline
- High Risk Termination Staffing
- Security Incident Tracking/Management

3 VIOLENT IDEATION

- Social Media/Threat Monitoring
- Violent Threat/Behavior Assessor
- Security Incident Tracking/Management
- Anonymous Reporting Hotline
- Security Investigation Services

4 RESEARCH & PREPARATION

- Structural Physical Security
- Visitor Management Systems
- Electronic Access Control
- Video Surveillance
- License Plate Readers
- Security Incident Tracking/Management
- HELIAUS® AI Workforce Management Tool
- Security Staff
- Hostile Surveillance Detection
- Canine Weapons Detection

5 ARRIVAL AT SITE

- Structural Physical Security
- Electronic Access Control
- Intrusion Detection/Alarms
- Video Surveillance
- HELIAUS® AI Workforce Management Tool
- Remote Alert/Alarm Monitoring
- Gunshot/Sound Detection
- Canine Weapons Detection
- Electronic Weapons Detection

6 COMMITS ASSAULT ACT

- Security Operations Center
- Allied Universal® MaRC Remote Monitoring
- Electronic Access Control
- Video Surveillance
- Gunshot/Sound Detection

7 RETREAT / NEUTRALIZATION

- Video Surveillance
- License Plate Readers

PREPAREDNESS MODEL SECURITY SOLUTION GLOSSARY

ALLIED UNIVERSAL® MaRC REMOTE MONITORING

A virtual SOC can provide all of the benefits of a physical SOC in the event that local law enforcement responds to an event. The remotely managed virtual SOC, however, can be accessed in a more mobile fashion, through the rovision of access to information and systems through a mobile device or laptop that can be used wherever the first responders designate as their incident command location.

ANONYMOUS REPORTING HOTLINE

Threat reporting hotlines allow employees to anonymously voice concerns without fear of retaliation. Reporting is a critical part of any workplace violence prevention program.

CANINE WEAPONS DETECTION

Firearms and explosive detection canines can detect a weapon in situations where metal detection is not available. Facility sweeps with canines can also uncover weapons or explosives that have been hidden on-site in advance of a planned assault.

Detecting a threat actor's attempt to enter a site with a weapon is another barrier to their ability to conduct an attack. Firearms detection canine teams can provide both the detection and initial response to reduce the likelihood of any person carrying a concealed weapon into the environment. They can also provide a visible deterrent to the threat actor prior to an attempt.

Local enforcement will be the main line of response, but even here, certain security tactics can assist in making that response even more effective.

ELECTRONIC ACCESS CONTROL

Technology systems with embedded analytics are truly excellent at the type of pattern and anomaly recognition needed to identify someone who is in the research and preparation phase.

When individuals are actively planning an assault, they often test or probe the security program to determine the actions they can take that will or will not result in a security response (example — entering unauthorized areas, attempting to access outside of hours) Analytics on electronic access control can identify outof-the-ordinary patterns of behavior or access attempts inconsistent with role policy. These patterns may be escalated to the threat management team for assessment.

During an active assault event, limiting access to additional victims can be facilitated through remotely managed and controlled access/locking devices on doors throughout a site. Locking doors can close certain areas of the site to the threat actor and help responders to separate the threat actor from potential victims.

ELECTRONIC WEAPONS DETECTION

Metal detection, coupled with security gates, can provide a highly automated way to deny access to a site by persons who are attempting to carry firearms into an area.

GUNSHOT/SOUND DETECTION

Like video surveillance with analytics, sound detection is a security control that can assist in detecting crisis-related activities such as gun shots, shouting or screaming that is outside of a certain set decible range, breaking glass, or other identified sounds that might indicate a threat actor is attempting to access a site using a weapon. Alerts from these analytics can be routed to responders for quicker awareness of any events in progress and expedite assessment of and response to the activity.

EMERGENCY RESPONSE PLAN CREATION, TRAINING AND EXERCISES

Emergency response plans that are in place and well-trained and socialized can help reduce harm of an active event. Training and exercising are the main path to ensuring that in any crisis, those responsible for action understand how to respond and can do so based on practice and repeated exposure to the scenario.

HELIAUS® AI WORKFORCE MANAGEMENT TOOL

Speed of response is a key factor in limiting harm in an active assault scenario. By enhancing security personnel's ability to send panic alarms, report suspicious activity or intrusions more quickly, and be sent direct response tasks in the event of a crisis, HELIAUS allows the on-site security responders to quickly and effectively escalate situations to local law enforcement for appropriate response.

In addition to the benefits of any technical / alarm incident tracking, HELIAUS adds the ability to report incidents or out-of-place behavior as it is witnessed by the security professional on site and with photographic evidence that may be used in further actions such as BOLO reporting.

HIGH RISK TERMINATION STAFFING

Terminations are often cited as the "grievance event", although sometimes a termination is the result of a pattern of poor behavior based on some other grievance. High risk terminations are those that the threat management team determines might be a trigger point for a violent reaction. Planning for these events and augmenting the security presence can assist in maintaining calm during these events.

HOSTILE SURVELLIANCE DETECTION

A Hostile Surveillance Specialist (HSS) covertly analyzes potential threats and hostile activity, stopping threats before they manifest. On-site hostile surveillance specialists monitor critical surveillance areas for hostile activity and quickly ascertain the nature of any and all threats. The covert nature of this type of security professional allows them to identify behavior and patterns that a threat actor might take care to hide in the presence of visible security or other authority figures of the organization.

INTRUSION DETECTION/ALARMS

Intrusion detection systems and associated alarms alert security responders to attempts to access through non-standard entrances. Intrusion detection can be placed on fences, windows, exit-only doors, and other areas where physical, visual, and auditory sensors can alert to unauthorized activity.

LICENSE PLATE READERS

Although many active assault events end with the apprehension of the threat actor, the need for evidence and documentation to identify an assailant that flees the site or to investigate and prosecute the event is a critical part of ensuring that further threat from the same threat actor is reduced. Additionally, the vehicle information provided to law enforcement can assist with identification and apprehension in the event that a previously unknown or unrecognized assailant flees the scene.

SECURITY OPERATIONS CENTER (ON-SITE OR OFF-SITE DEDICATED) During any active crisis, speed of response, availability of information, and communication are key factors in rapid and effective response. A dedicated security operations center that monitors all of the on-site electronic security systems can allow first responders to access the

video, access, alarm, and other analytics from the site to enhance the effectiveness of the emergency management process. With a SOC in place, especially one with virtualized interfaces that can be run from any laptop, law enforcement can have the ability to review and control the crisis event.

SECURITY STAFF

Technology cannot address all vulnerabilities. As humans, we often have an innate sense when things are amiss and can identify and report on suspicious activity.

On-site security staff provides a consistently visible reminder to any potential threat actor attempting to identify targets, that the site is under surveillance and is able to quickly respond to threatening actions. A strong and visible security presence can often deter threat actors from taking any actions that they deem too risky.

SOCIAL MEDIA MONITORING

When individuals are moving along the path to violence, they often engage in what is called “leakage”, which, in the context of threat assessments, is the communication to a third party of an intent to do harm to a target. The means of communication may vary and include letters, diaries, journals, blogs, online videos, emails, voice mails, and other digital forms of transmission. Leakage is a warning behavior that typically implies a preoccupation with the target and may signal the research, planning, and implementation of an attack.

Social media is a common outlet of leakage and monitoring it is one way to identify and escalate indicators of the intentions of threat actors.

STRUCTURAL PHYSICAL SECURITY

Structural physical security and environmental design that promotes security goals are often the first and least costly methods to deter threat actors from entering a facility.

If early detection and threat management activities do not deter the escalation to violence, the on-site physical security infrastructure and controls are key to limiting the access of the threat actor to the site and limiting access to intended victims. Beginning with basic physical security infrastructure such as perimeter fences to limit site access, gates that effectively stop unauthorized access and traffic, and hardened and properly secured doors will ensure that any threat actor has limited physical access to the site and potential victims. Reduction of harm is the key at this point.

THREAT / VULNERABILITY ASSESSMENT

This is the foundation of preparedness. A comprehensive threat assessment is vital to understand two aspects of risk. 1) The likelihood of an active assault on the facility and 2) any gap areas that could be exploited to engage in an assault. A thorough assessment in today’s environment also looks at the online / virtual presence of the organization, as well as environmental factors to understand likelihood, and follows through with a deep dive into the existing facility security. If there is no understanding of the vulnerabilities, then it’s essentially impossible to properly mitigate those gaps.

VIDEO SURVEILLANCE

Video surveillance with facial recognition analytics can assist in identifying individuals that have been identified as threats or individuals that have been prohibited from a location. Analytics can also be used in investigations of unidentified or unauthorized activity in sensitive areas.

VIOLENT THREAT / BEHAVIOR ASSESSOR

Well trained threat management teams are critical to identifying potentially violent individuals in the workplace. The addition of a professional independent psychological evaluator to conduct clinical violence risk assessments when necessary helps the threat management team ensure that their initial assessment is correct or provide additional insight into why an individual who is displaying some concerning behaviors may not pose a threat to the environment after all.

Having an established relationship allows for a faster response when needed and can ensure any legal or contractual requirements are not an impediment to support in a time of need.

VIRTUAL THREAT ASSESSMENT

An assessment of the online / virtual presence of the organization helps understand what people are saying in the media and whether there might be a virtual threat to the enterprise in addition to any threats/vulnerabilities found in a physical security assessment.

VISITOR MANAGEMENT SYSTEMS

Control and management of visiting/non-credentialed individuals on a site is critical to maintaining control over potential threat situations.

WORKPLACE VIOLENCE AWARENESS / PREVENTION CAMPAIGN

Creation of workplace violence awareness and prevention programs such as the “See something. Say something” campaign helps identify threats in the workplace. The people most likely to interact with a person who has experienced a grievance event, or has internalized a perceived social threat and made it a personal grievance, are those who engage with that person every day. Awareness and understands that reducing violence is everyone’s responsibility is a force multiplier of the mitigation impact of the threat management team. Being aware of potential threats allows the threat management team to help move potential attackers away from the path to violence.

WORKPLACE VIOLENCE PREVENTION POLICY / THREAT MANAGEMENT TEAM

Workplace Violence Prevention Policy and Procedure combined with Threat Management Team is another critical pre-threat mitigation activity. As part of an overall workplace violence prevention program, the threat management team learns to recognize and manage the causes, signs, and vulnerabilities to acts of many different types of workplace violence.

Putting a team in place responsible for managing threats and providing them with the right policy, procedure, and training goes a long way to positioning the organization to effectively identity, assess, and then take actions to move potential attackers away from the path to violence.

ALLIED UNIVERSAL®

There for you.

Allied Universal®, There for you.®
There for you®, serving and safeguarding customers, communities, and people around the world.

How Can We Help?
Allied Universal® specializes in helping organizations improve their state of readiness and security by taking a comprehensive approach to addressing emergency preparedness, workplace violence awareness and prevention, and response to active shooter and active assailants. Our integrated solutions not only to identify risks and vulnerabilities but also help to close security gaps and place organizations on a pathway to resilience.

Contact us to learn more.

www.aus.com