SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices> Protecting People >

Active Shooter Program: First Steps

By the Security Executive Council

When tragedies like the May 2022 Uvalde, Texas, school shooting grip the national psyche, news outlets often connect the dots with similar events, implying trends in frequency or severity of incidents that aren't always backed up by data.

Unfortunately, in this case, the pundits aren't wrong.

A May 2022 report by the FBI indicated that active shooter incidents in the US increased more than 50% from 2020 to 2021, and deaths attributable to these incidents hit their highest number since 2017. The events occurred across 30 states in a variety of facilities, including schools, churches, government properties, healthcare facilities, gas stations, supermarkets, spas, and shipping facilities.

Security leaders and executives have been paying attention. Our clients have increasingly contacted us for information on creating formal programs to manage active shooter threats, sometimes at the request of their boards of directors. Here are our recommendations for how to begin the process.

As with any type of new program, your first step should be ensuring you understand your company's goals in requesting this program, its organizational needs, risk appetite, and your Current Conditions, Circumstances, Culture, and Resources (your operating environment, or what we call your C4R™). If you don't feel clear on any of these elements, stop now and take a look at a few of our other resources:
The OPAL+ Assessment
How Firm Is Your Security Foundation?

If you're confident in your knowledge of the company, consider the steps below as you develop your active shooter program.

1. With this type of risk, the possibility of post-incident litigation must remain front of

mind as you begin program development. Review all legislation, regulations, industry standards, and voluntary compliance programs, and incorporate the elements that are appropriate for your company as your baseline.

There are currently no federal laws or regulations that govern how all U.S. companies respond to active shooter incidents. However, there are several standards that may apply, and plaintiffs' attorneys will be ready to point that out should an incident occur. (Click here for more on how to ensure your security programs are defensible in court.)

Check with the standards bodies that most frequently release security-related standards, including ANSI, ISO, NFPA, BSS, and ASIS. Some of the existing standards that are relevant for active shooter incidents are:

- NFPA 3000: A Standard for an Active Shooter/Hostile Event Response (ASHER) Program. Current Edition 2021. This standard addresses all aspects of the process, from identifying hazards and assessing vulnerability to planning, resource management, incident management at a command level, competencies for first responders, and recovery.
- ASIS WVPI AA-2020: Workplace Violence and Active Assailant – Prevention, Intervention, and Response Standard. Published in 2020. This standard includes 120 elements to review and consider. In my opinion, some of the included elements are inappropriate, and this standard could cause companies significant legal risk. Use with care.
- NFPA 1616 Standard on Mass Evacuation, Sheltering, and Re-Entry Programs. Current Edition 2020. Is applicable to event security, emergency response, crisis management and business continuity programs as well.
- NFPA 1600 Standard on Continuity, Emergency, and Crisis Management. Current Edition 2019. Widely used by organizations of all types, NFPA 1600 has been adopted by the U.S. Department of Homeland Security as a voluntary consensus standard for emergency preparedness.

2. Once you have digested these standards and chosen your basic program elements, you may want to consider having your legal department pull up the relevant case law for workplace violence, event security, and mass shooting cases and give you a legal opinion on the company's most significant liability risks the program should address.

3. Next stop is your insurance carriers and underwriters. In response to high-profile incidents like the MGM shooting and the Houston concert tragedy, insurance carriers are requiring a number of new security, risk assessment, and emergency response items that you will need to incorporate. These measures could reduce both exposure and cost.

4. Once you have completed the steps above, review your findings and recommendations with Legal, HR, Event Management, Risk Management, Insurance, and Compliance. Their input will round out your baseline program.

5. Document your program and related processes clearly and meticulously to maximize effectiveness and minimize liability.

The SEC can help with any or all of the steps in this process. Contact us to discuss how we can assist you.

Visit the Security Executive Council web site to view more resources in the Program-best-practices/Protecting-people series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

