WHITEPAPER

Reducing the Risk to Critical Infrastructure with Gunshot Detection

Shooter Detection Systems™

AN ALARM.COM COMPANY

THE ACTIVE SHOOTER THREAT

In the United States today, active shooter incidents are a persistent threat with a concerning pattern of elevation. According to the FBI, the number of such incidents per year spiked in 2021—at the height of the Covid pandemic—and has since declined somewhat, but it has not returned to pre-pandemic levels. The FBI recorded 48 active shooter incidents in 2023, the most recent statistics available, marking an increase of 60% in the annual number of these events since 2019.

Many of these attacks target businesses. According to data from activeattackdata.org, many active shooter attacks from 2000-2023 (approximately 43 percent) happened at places of business. In an FBI review of active shooter incidents in the United States from 2000–2019, more than a third of incidents occurred in businesses (137 out of 333). Recent legal rulings extending the right to purchase handguns, making it easier for employees to carry firearms or keep them in vehicles parked on company property, have the potential to exacerbate the crisis.

CRITICAL INFRASTRUCTURE IS VULNERABLE TO ATTACKS

Critical infrastructure businesses such as airports, power plants, public utilities, food processing, and data centers are particularly vulnerable to the disruptions of an active shooting incident and appear to be attractive targets for shooters.

> ***There's a lot of chatter on the dark web and the nefarious parts of the internet where people are planning to attack and destroy critical infrastructure.***
>
> 
>
> **- Brian Harrell, former Assistant Secretary for Infrastructure Protection, DHS and first Assistant Director for Infrastructure Security, CISA**

In 2022, intruders fired at two of Duke Energy's electrical substations in Moore County, North Carolina, causing damage that cut off power to 45,000 people. Another high-profile incident in recent memory was the 2013 sniper attack on Pacific Gas and Electric's Metcalf station in Northern California, which took out 17 transformers and spawned new mandatory Federal Energy Regulatory Commission (FERC) physical security standards for substations.

"There's a lot of chatter on the dark web and the nefarious parts of the internet, where people are planning to attack and destroy critical infrastructure," says Brian Harrell, SDS's National Security Subject Matter Expert (former Assistant Secretary for Infrastructure Protection at the U.S. Department of Homeland Security and first Assistant Director for Infrastructure Security at the Cybersecurity and Infrastructure Security Agency). "For example, right now, the power grid is very visible, but I think these concerns also apply to water systems, financial systems, and maritime port facilities."

BUSINESS REPERCUSSIONS

Attacks on critical infrastructure have almost unimaginably wide-ranging repercussions, for public well-being and national security as well as business operations.

In addition to the immediate and traumatic human impacts of loss of life, injury, and psychological distress, which are foremost in the minds of any CSO or board, the following impacts to the business may occur:

Loss of Business Continuity

Regular operations are interrupted, potentially for a prolonged period of time as the facility becomes a crime scene and is shut down during the investigation process. Revenue is lost while business is suspended, and reopening costs may be incurred.

Interruption of critical services to the public

Whether the business is a transportation center, a power plant, a data center, or a public utility such as water or gas, the surrounding community may be inconvenienced or worse. For example, the 2022 Duke Energy attack left 45,000 people without power for almost a week (including an 87-year-old woman who died when her oxygen machine stopped functioning as a result of the outage).

Costs incurred for repairs and additional security measures and infrastructure

For example, the 2013 Metcalf attack caused an estimated $15 million in damage and PG&E spent $300 million to protect substations following the incident.

National security implications

Critical infrastructure facilities such as airports, nuclear plants, and data centers may be closely tied to the essential functions of government and interruptions in their operations may pose security risks.

Reputational damage

In the aftermath of an active shooter attack the board, and the public, may lose trust in the affected entity's abilities to operate and to maintain a safe facility.

Increased regulatory scrutiny

Investigations that follow active shooter attacks may lead to additional regulation of the business and/or industry. The Metcalf attack, for instance, resulted in the passage of new legislation directing the California Public Utilities Commission to address physical security risks to the distribution system of California's electric corporations.

Liability

Businesses targeted by active shooters are frequently sued after the incident, as was the case with MGM Resorts International in Las Vegas after a 2017 mass shooting there. The U.S. Occupational Safety and Health Administration (OSHA)'s General Duty Clause requires employers to protect their employees against "recognized hazards likely to cause serious injuries or death," and businesses are encouraged to develop policies on active shooter response and to show that they have taken all possible measures to safeguard their facilities.

In the aftermath of an active shooter attack the board, and the public, may lose trust in an organization's abilities to operate and to maintain a safe facility.

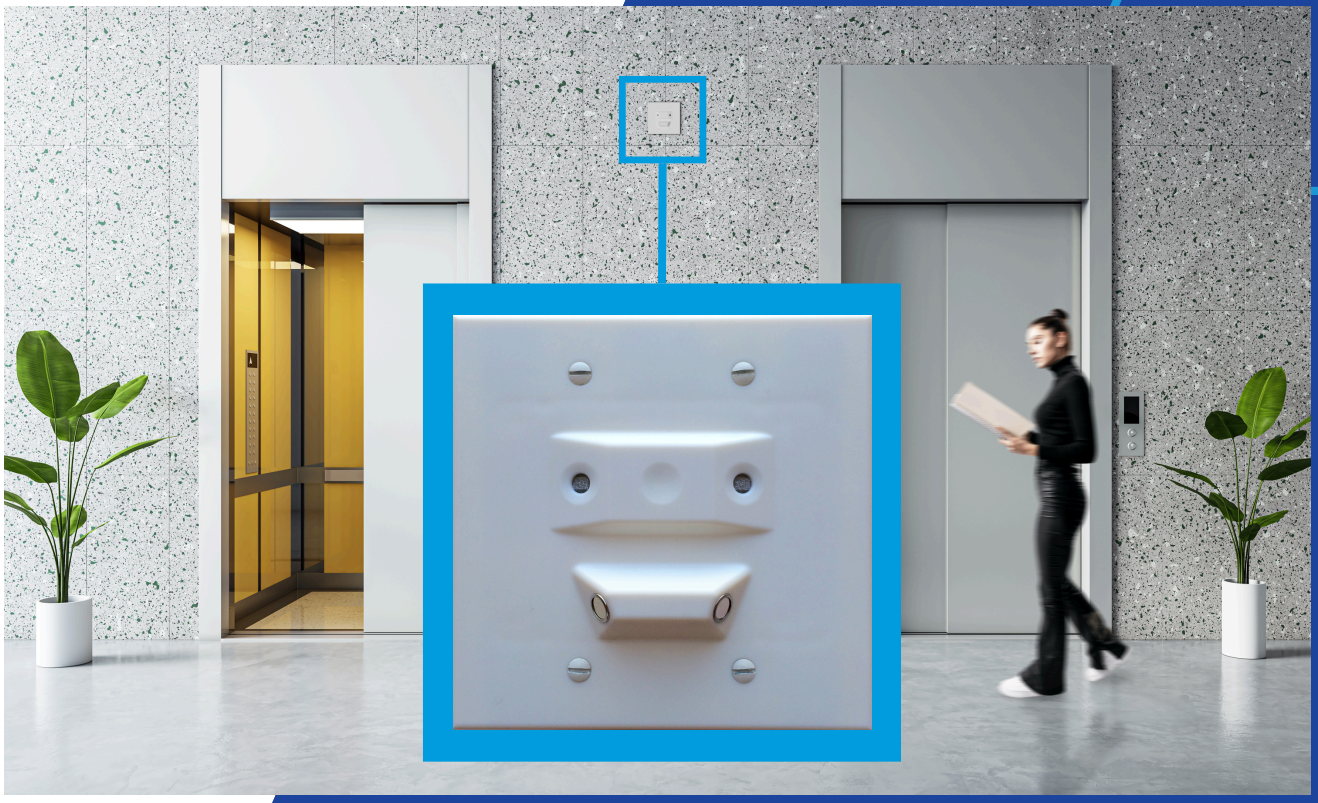
WHAT CAN BUSINESS LEADERS CONTROL?

What can the CSOs and boards of critical infrastructure businesses do to minimize the above impacts, in the event of an active shooter incident? Although it is difficult to plan for this type of extreme attack conducted by a determined adversary, one way to do so is to take measures to ensure that information during any such event will be communicated in real time and that emergency responders will arrive on the scene as quickly as is possible. Gunshot detection technology by Shooter Detection Systems (SDS), which links fast and accurate gunfire-detecting sensors to other security systems and uses automation to speed first response and mitigation, is one such solution.

"When seconds count, we need to ensure that our response is quick, efficient, and accountable to our staff, our customers, and to the people that we love and care about," Harrell says. "When the after-action report comes out, and when the media, public commissions, and elected officials ask their questions, we want to be able to say that we took this threat seriously—we protected our people, and we made the right investments in risk reduction."

SDS was the first company to bring gunshot detection technology to the commercial market and, although other gunshot detection products have since been introduced, remains a proven leader in the field. Its dual-factor sensors, which pick up both the acoustic wave of a gunshot and the infrared signature of a muzzle flash for unparalleled accuracy, were adapted from a U.S. military sniper detection system called Boomerang that was used to protect troops under fire from insurgents during the Iraq War and is still in use today.

Placing gunshot detection sensors inside and outside of facilities is a security measure that puts an organization in control of detection of and response to shooting incidents.



**- Jin Kim, FBI (Ret.)
Active Shooter Subject
Matter Expert**

In this age of artificial intelligence-driven, video object recognition solutions, trained personnel are still required to identify threats, intervene quickly, and communicate effectively during periods of extreme stress and confusion.

Fully autonomous gunshot detection, tracking, and notification systems change this dynamic. Removing human emotions, reactions, and assumptions from the equation significantly improves the intra-event response for those under attack."

GUNSHOT DETECTION SYSTEMS AND CAPABILITIES

Gunshot Detection by SDS offers the following capabilities, which can significantly reduce risk to critical infrastructure businesses:

Speed: SDS detects gunfire and sends real-time alerts within half a second, reducing the time to mitigation. According to SDS advisory board member and active shooter subject matter expert Jin Kim, a 23-year veteran of the FBI's New York division: "Time is absolutely critical. Time is the biggest commodity that an average human being has in these events."

Accuracy: SDS's product detects gunfire with 99.9 percent accuracy, with less than one false alert per five million hours of sensor use—nearly eliminating the possibility of a false alarm. Such events can be very costly and disruptive, and in the case of a critical infrastructure facility open to pedestrian traffic they can even cause mass panic (as was the case with an active shooter scare at JFK Airport in 2016). A multi-agency security review of that incident found that "the danger posed by a panicked mass of people fleeing for their lives cannot be overstated."

Seamless integrations: Seamless integrations: SDS gunshot detection works in concert with other security systems such as video, access control and mass notifications. This enables security teams to quickly lock down the facility, use its cameras to track the shooter, and notify building occupants via emergency alerts and local alarms.

Automation: Unlike competing solutions based on video technologies, which typically require additional verification by a human in the loop, SDS gunshot detection is fully automated—speeding the alert process and eliminating the human-error factor.

Expedited first response: SDS transmits precise location information to first responders, with visual mapping that allows them to see in real time where the gunshots are occurring as well as the shooter's path through the building. Responders can proceed directly to the locations where they are most urgently needed.

Privacy: At a time of increasing concern about the storage and transmission of personal information and proprietary data, CSOs and boards may appreciate that SDS gunshot sensors do not record or stream audio (unlike some competing products on the market). Microphones are tuned only for high-decibel sounds, no audio leaves the sensor, and all processing is done at the edge.

ADVANCE PLANNING FOR ACTIVE SHOOTER THREATS

Although an active shooter event is the type of unthinkable, catastrophic situation that can make even the most experienced security professionals feel powerless, the addition of industry-leading gunshot detection technology by SDS to a comprehensive security portfolio allows CSOs to state with confidence that they have done everything possible to reduce the risks of such an event should it occur.

This advance planning is particularly important for businesses in the critical infrastructure sector, which are under increasing threat and face unique vulnerabilities and liabilities. According to SDS's National Security Expert Harrell, "This technology is going to be a force multiplier for all critical infrastructure."

SOURCES:

ActiveAttackData.org
FBI 2023 Active Shooter Report
FBI 20-Year FBI Review
ABC News
ScotusBlog.com
Governor.NY.gov
WRAL News
Marketplace.org
Washington Post
California Public Utilities Commission
OSHA Workplace Violence Reinforcement
National Public Radio

Visit ShooterDetectionSystems.com to learn how our indoor and outdoor gunshot detection systems can help you protect your infrastructure and your people.

Shooter Detection Systems™

300 Newburyport Turnpike

Rowley, MA 01969

Email: sales@shooterdetectionsystems.com

Phone: 1-844-SHOT911

www.ShooterDetectionSystems.com