SHRM.org

How to Spot Potential Attacker Red Flags

Sara Mosqueda

October 6, 2023

Even when law enforcement's response to an active shooter is flawless and entirely by the book, the attacker can still leave behind injuries or deaths.

The Metro Nashville Police Department's officers were praised for quickly ending a mass shooting in April 2023 at a private parochial school. Officers responded in less than 15 minutes from the initial 911 call reporting an active shooter. Yet the community was still harmed by the deaths of the three staff members and three students.

But just how did the attacker go undetected until that day? Is any attack unexpected? Research shows that people don't just become active shooters or attackers in a snap. Instead, it's a decision.

"Right now, it seems like we're completely focused on the response to these incidents," said Joshua Shelton, a senior security specialist at FedEx in Atlanta. "The problem is…you can't do something until you hear the 'bang.' Action is always faster than reaction."

Main Takeaway

Part of the prevention process demands an awareness of the indicators that signal someone has started walking down the path towards orchestrating a violent attack. There are six trail markers on this path: grievance, ideation, research of the intended target, preparation, breach and the attack itself.

These steps are fluid—for example, if someone is prepared and ready to attack but is surprised by an aspect of his or her target, it could just be a temporary setback to conduct more research. This was the case last month in Jacksonville, Florida, when a seemingly unarmed man approached Edward Waters University but was asked to leave when he refused to provide identification to a campus security guard. Some setbacks can push a planned attack back for days, weeks or months. This one was minor, however, as the man then traveled to a nearby store and shot and killed three Black people.

This pathway to violence, especially among employees, is only one of eight red flags—more formally known as proximal warning behaviors. The other flags are fixation, identification, novel aggression, energy burst, leakage, last resort and direct threat.

"There are lots of risk factors. These are the big ones, though," Shelton said. "These are the flashing lights that let us know if people in our employ are doing these things, we have got to be doing something about them."

Based on years of research from scientists and academics that identified these warning signs, Shelton explained that the ones that indicate the greatest level of risk are the pathway, identification and last resort.

Identification is defined as when a developing attacker takes on the persona of a warrior for a specific cause. This person may "feel justified in their action because they are so angry. They take on this attitude that they are going to be a warrior for their cause and carry out this justified attack," Shelton said. Sometimes this can be spotted with paraphernalia or militarized clothing that contrasts the person's previous aesthetics.

The last resort indicator is one generated by both a potential attacker and the people that influence his or her life: family, employers and figures of authority. Quite simply, when someone senses there is no escape or no other answer, the resulting desperation can increase their risk of harm to others.

"We all learn early on not to corner an animal, and humans are no different," Shelton said.

Next Steps

Once you know the warning signs, it helps to have others in your organization recognize them, too.

Threat assessments, which should not be confused with profiling, can deliver a greater level of successfully mitigating an attack when multiple stakeholders from within an organization are involved. At the very least, representatives from security, human resources, legal and operations should be involved as a team in these assessments, which can be used to manage concerning behaviors. "This is not a single-silo job," Shelton emphasized.

Once everyone puts egos aside and focuses on the shared goal of reducing the lethality of any scenario, they can identify which elements are under their control and begin to create a plan for how to assess a possible threat.

Shelton recommended an educated approach to the threat assessment process, including understanding how to apply certain interventions and the use of well-established tools, such as structured professional judgment instruments. This would include, for example, the *Workplace Assessment of Violence Risk* by Stephen White and Reid Meloy.

At the core of these processes—from investigation to resolution—is the need to identify a threat based on its behaviors.

Sara Mosqueda is associate editor of Security Management *magazine.*