

Trends and Recommendations: Workplace Insider Homicides, 2000–2025

VIOLENCE
PREVENTION
PROJECT

RESEARCH CENTER

HAMLINE UNIVERSITY

James Densley and Jillian Peterson, cofounders of the Violence Prevention Project

Most workplace killings in the United States are robberies perpetrated by strangers against convenience store clerks, taxi drivers, late-shift retail workers, and others. However, little is known about the number of workplace killings committed by current or former employees. Most workplaces have developed security measures (e.g., cameras, locked entries, panic buttons) designed for *outsiders*, not insiders. This brief focuses on the homicide risk posed by current or former employees and how workplaces can mitigate it.

Key Takeaways

What to know

- 94 percent of perpetrators walked into the workplace using their existing credentials.
- 60 percent of incidents were preplanned.
- 20 percent of victims were supervisors or managers.
- 24 percent of perpetrators were reprimanded before the attack.
- 50 percent of perpetrators showed warning signs before the attack.

What to do

- Build confidential, nonpunitive reporting systems.
- Establish workplace threat assessment teams.
- Treat termination and discipline as high-risk events.
- Train staff on warning signs, deescalation, and suicide risk recognition.
- Make Employee Assistance Programs genuinely accessible.
- Build a continuous signal system.
- Plan for the post-termination window.

The DVERT Center is supported by the National Institute of Justice, Office of Justice Programs, US Department of Justice under Award No. 15PNIJ-24-GK-00750-DOMR. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors, and do not necessarily reflect those of the Department of Justice.

In this brief, we draw on the Violence Project's Database of Workplace Insider Homicides, which includes 653 incidents at US workplaces from 2000 to 2025 committed by perpetrators who were current or former employees.* We describe the broad patterns, treat active shooter incidents as a distinct subset (defined, per federal guidance, as one or more people actively engaged in killing or attempting to kill others in a populated area), and offer recommendations for human resources leaders, security directors, workplace threat assessment teams, and managers.

Workplace insider homicides

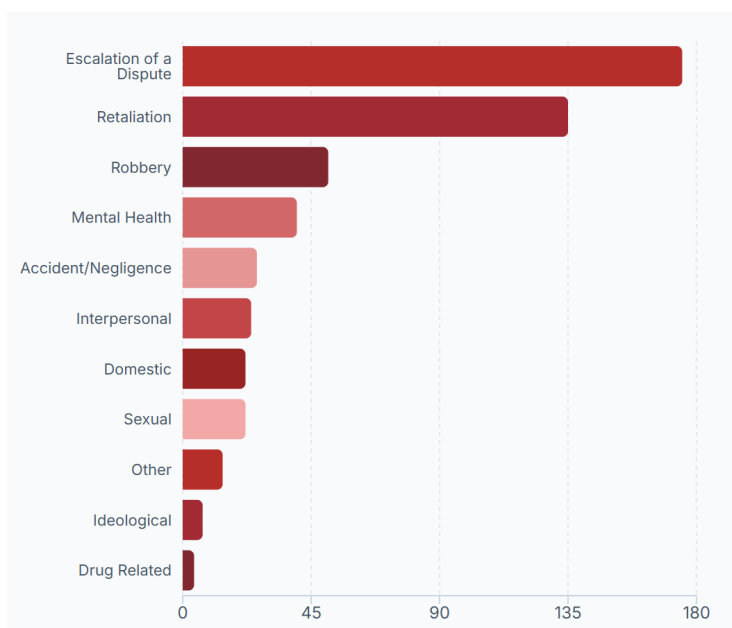
According to the database, 653 workplace insider homicide incidents occurred in the United States between 2000 and 2025, resulting in 920 deaths. Food and drink establishments accounted for 19.9 percent of incidents, and manufacturing accounted for 13.5 percent. Together, these two industries represent around a third (33.4 percent) of all cases. Both sectors feature long shifts, thin supervision margins, and open access to back-of-house areas.

Incidents clustered in December and June, with Tuesday being the most common day of the week. Nearly three-quarters of incidents (71.6 percent) occurred indoors. Crucially, 94 percent of perpetrators walked into the workplace on credentials they already had. As a result, efforts to harden buildings, strengthen perimeters, and manage visitors would not have prevented these incidents because the killer was already inside.

Firearms were used in 67 percent of cases. Knives accounted for 15.9 percent. In addition, 59.9 percent of incidents were preplanned rather than spontaneous. Active shooter events accounted for 22.4 percent of cases (146 of 653 incidents).

The two most common situational drivers were escalating disputes (26.8 percent) and retaliation (20.7 percent). A *dispute* is an unplanned conflict that escalates quickly; examples include a shift-floor argument, a parking-lot confrontation, or a reaction to a denied promotion. In contrast, *retaliation* is a planned conflict that escalates over days or weeks.

Workplace homicide situations



Source: Jillian Peterson and James Densley, Workplace Homicides, Violence Prevention Project, 2026, <https://www.theviolenceproject.org/databases/workplace>.

* The numbers presented here describe the observed population of insider homicide perpetrators; we are not using these numbers to make a propensity claim about any group. The numbers should be understood within the context of industry composition, not national demographics.

Workplace insider victims

The 920 victims ranged in age from 11 months to 100 years, with an average age of 41.5. Most were male (74 percent). Racially, 53.6 percent were White, 26.7 percent were Black, 13.6 percent were Hispanic, and 4.5 percent were Asian. Three-quarters (74.3 percent) were killed inside the workplace itself.

Two-thirds of victims (67.0 percent) were coworkers of the perpetrator. Nearly a fifth (19.9 percent) were supervisors or managers, the second-largest victim category in the dataset. The implication of this statistic is that those in managerial roles are often deliberately targeted.

Perpetrators

The perpetrators ranged from 16 to 86 years old, with an average age of 36.6; the most common ages were the mid-to-late twenties. The perpetrators were overwhelmingly male (92.8 percent). Female perpetrators were concentrated in health care, which largely reflects workforce composition in that sector rather than a gender-specific pathway to violence.

The racial composition of the perpetrators was 45.2 percent Black, 33.3 percent White, and 15.1 percent Hispanic. That distribution is shaped heavily by the industry and by the location of the incidents. For example, food service, retail, and manufacturing all have workforce demographics that differ significantly from the US labor force as a whole.

Three-quarters of perpetrators (76.7 percent) were current employees at the time of the attack. Another 20.8 percent were former employees. Another 2.5 percent were owners. In the active shooter subset, that distribution shifts meaningfully toward former employees.

Nearly a quarter of perpetrators (24.1 percent) had been recently reprimanded. Another 27.3 percent had a known criminal history, 17.9 percent had a documented history of violence, 19.9 percent had a documented mental health history, and 28.9 percent had a history of suicidality. More than half (58.5

percent) had experienced a recent significant stressor outside of work, including divorce, financial crisis, housing loss, and bereavement.

Behaviorally, 50.5 percent of the perpetrators showed warning signs before the attack that were noticed by colleagues, supervisors, or family members. *Warning signs* are defined as behavioral shifts such as fixation on a grievance, paranoid statements, social withdrawal, sudden personality change, and escalating anger. In contrast, *leakage* refers to directly or indirectly communicating intent via threats, cryptic messages, or confessions to a friend. Of the perpetrators, 9.6 percent engaged in leakage. Because the leakage rate is considerably lower than the warning sign rate, workplaces that rely on only reports of explicit threats will miss other signals of danger.

Most perpetrators were arrested (76.3 percent), but 20.5 percent died by suicide at or near the scene. Another 2.9 percent were killed by law enforcement. The suicide rate suggests insider workplace violence sits at the intersection of homicide and suicide more often than most homicide categories.

Active shooter cases

Active shooter incidents accounted for 22.4 percent of all insider workplace homicides (Sample size = 146) and had characteristics that matter for prevention.

The perpetrators were older. The modal age was in the early forties, roughly 15 years older than the overall insider workplace homicide average. The perpetrators were overwhelmingly male (94.5 percent). Former employees were overrepresented (33.1 percent, versus 20.8 percent overall), suggesting that the post-termination period is a particularly high-risk window for the most lethal type of attack.

The incidents were more frequently planned. Of the incidents, 85 percent were preplanned compared to 60 percent overall. The incidents were also more concentrated on weekday mornings (43.8 percent), which aligns with shift starts. Manufacturing is overrepresented: 21.9 percent of active shooter incidents occurred in this industry compared to 13.5

percent of insider incidents overall. In contrast, the food and drink industry experienced 8.9 percent of such incidents compared to 19.9 percent overall.

Of the active shooter events, 12 percent (18 cases) involved assault weapons. Most occurred indoors (84.9 percent). Almost none (7.6 percent) involved forced entry. The perpetrator either already had access or walked in before anyone could stop them.

Retaliation drove 56.8 percent of active shooter cases, compared to 20.7 percent of insider workplace homicides overall, suggesting that these events were overwhelmingly planned retaliation for a perceived injustice at work, often amplified by a personal crisis.

Among active shooter perpetrators, 37.7 percent had been recently reprimanded (versus 24.1 percent overall), 35.6 percent had a documented mental health history, and 63.7 percent showed signs of suicidality. In addition, 80 percent had experienced a significant recent stressor, 69 percent showed warning signs, 16 percent leaked explicit intent, and 15 percent left a legacy token (i.e., a note, manifesto, social media post, or video meant to be discovered after the attack).

Nearly half of active shooter perpetrators (49.7 percent) died by suicide. Another 9 percent were killed by police. Only 41.4 percent were arrested. In more than half of these incidents (58.2 percent), the perpetrator did not intend to survive.

Example cases

In each case in the following list, a different warning-sign pattern was visible in the weeks or hours before the attack:

- **Unusual behavioral shift.** A man entered the manufacturing plant where he worked armed with a shotgun and opened fire. He killed his supervisor, shot himself four times, and then was killed by responding officers. In the weeks beforehand, coworkers noticed he had been “acting funny.” Normally cheerful and helpful, he had become forgetful and unable to finish basic tasks. He had not slept in three days. After an altercation with another employee over a female

coworker, he was asked to leave the premises, but he threatened to return with a gun. He came back once and was sent away again. He came back a second time armed.

- **Untreated serious mental illness.** A man diagnosed with paranoid schizophrenia believed his father and coworkers were conspiring with a Mexican cartel to kill him. He had stopped taking his medication three months before the attack. On the morning of the shooting, he called his family’s lawyer to ask whether he would defend him “if he had to do something to defend himself.” He then called the security guard at his workplace (an auto shop) to warn of a possible shooting and asked that a coworker (one of the eventual victims) be escorted off the property. He shot and killed his father, two coworkers, and a customer.
- **Termination ambush.** After several reprimands for using his phone at work, a plastics company employee was removed from the building by his supervisor. He went to his car, retrieved a gun, and returned. He shot the supervisor outside first, walked inside, and shot five more people before killing himself. Two hours before the attack, he had phoned his girlfriend and threatened to kill the supervisor and himself. She told police later that he had made similar threats before but she had not believed him.
- **Long aftermath.** An engineer, fired from his job and collapsing under divorce, unemployment, foreclosure, and bankruptcy, returned to his former workplace and shot six people, killing one. A neighbor had noticed he was disheveled in the weeks before; he had sat outside in his SUV for hours playing classic rock, and he had stared at her from his yard. He pled guilty, went to prison, and died by suicide there seven years later.
- **Ignored complaints.** A school custodian shot and killed his coworker and supervisor at the arts school where he worked; he then fled to Mexico. He had a documented history of workplace confrontation, intimidation, and threats of violence. One of the eventual victims had told administrators he feared for his life. Other

custodians had refused to work shifts with him because they were afraid of him. The complaints were on file. The custodian kept his job until the day of the killing.

- **Post-suspension return.** A Walmart employee of 20 years was suspended after pulling a knife on a coworker during a dispute. Three days later, he returned to the store, opened fire, killed two employees, and wounded a responding police officer. He was convicted of capital murder and sentenced to death.

Two patterns run through these cases. First, before every attack, a behavioral shift was noticed by someone (e.g., a coworker, a supervisor, a neighbor, a girlfriend, a family lawyer, a fellow custodian). Second, the behavioral shift was almost always recent, and the deterioration was legible to the people around them.

Recommendations

The following recommendations are tied to specific empirical findings in the data:

1. Build confidential, non-punitive reporting systems.

Reporting systems work when employees trust them. Systems should have multiple access points, including anonymous channels, a digital portal, and an in-person option. They should specify what kinds of behavior are worth reporting, including fixation on grievances, sudden personality changes, escalating paranoia, threats (however vague), and concerns about a colleague's mental state. The system should then tell the reporting employee that the concern is being taken seriously without breaching confidentiality; such follow-up will keep the system functioning across time. Given that only 1 in 10 perpetrators leaked explicit threats, reporting prompts should focus on broader behavioral signals, not just threats.

2. Establish workplace threat assessment teams.

Workplace threat assessment teams should be cross-functional and consist of human resources

personnel, security staff, legal counsel, behavioral health professionals, and members of senior management. They should function as proactive problem-solving groups that manage cases over time, not as after-the-fact crisis responders. Because insider risk tends to build over weeks and months rather than minutes, a case management mindset is essential. When legal or behavioral thresholds are met, teams should coordinate with local law enforcement and mental health providers; as available, they should initiate Extreme Risk Protection Order processes. Note that one in five insider perpetrators, and one in two active shooter perpetrators, died by suicide; therefore, workplace violence prevention is suicide prevention and vice versa. Programs that silo the two miss the common factor, which is a distressed employee who has lost hope and concluded that someone at work is responsible for their pain.

3. Treat termination and discipline as high-risk events.

Given that a recent reprimand appeared in roughly a quarter (24.0 percent) of all insider homicides and nearly two-fifths (37.4 percent) of active shooter cases, discipline and termination should be treated as operationally sensitive moments. The way discipline is administered (i.e., the timing, the tone, the surrounding support, and the exit protocol) is a safety consideration. To this end, the employer must explain why a decision was made, apply rules evenly, and treat the employee with dignity even when the news is adverse. The employer must also plan for high-risk cases through pre-termination risk screenings, thoughtful timing, clear communication of next steps, continuation of benefits when possible, referral to mental health and employment resources, and security awareness on the day itself. The goal is not to assume every fired employee is dangerous; rather, the objective is to recognize that the small minority who are dangerous often act within days of the termination.

4. Train staff on warning signs, de-escalation, and suicide recognition.

Half of all insider perpetrators showed warning signs, but fewer than 1 in 10 leaked explicit intent. As a result, programs that encourage reporting of explicit threats will catch only a minority of cases. The more useful signal of risk is behavioral change, including fixation on grievance, paranoia, isolation, and sudden drops in work quality. Staff should be trained to recognize such shifts through training that is scenario based, repeated, and calibrated to their roles. At minimum, three tiers of training are needed: general staff training on warning-sign recognition and reporting; frontline de-escalation training for employees who handle difficult interactions (customer service, health care, front desk, security); and deeper training for supervisors and managers on documentation, escalation, high-risk conversations, and response. Because insider violence and self-harm overlap so heavily, suicide prevention should be integrated into every tier rather than taught as a separate module.

5. Make Employee Assistance Programs genuinely accessible.

Nearly 6 in 10 insider perpetrators and 8 in 10 active shooters had experienced a significant recent stressor outside of work, including divorce, financial collapse, housing loss, and bereavement. Workplace grievance alone is usually insufficient. The highest risk cases resulted from a workplace grievance plus a life crisis. Workplaces that support employees through personal crises are investing in a known protective factor. Employee Assistance Programs (EAPs) are excellent resources that are widely offered; however, they are underused because of stigma, fear of employment consequences, and lack of awareness. Workplaces should treat EAPs as routine support infrastructure and promote them openly, especially during periods of institutional stress (e.g., layoffs, reorganizations, mergers,

major leadership changes). Leaders should be trained on how to suggest EAP resources without making an employee feel singled out or targeted. Offering EAP support to an employee experiencing a personal crisis may be among the most useful upstream interventions any employer can offer.

6. Build a continuous signal system.

Workplace climates are not static. To identify areas of rising tension before they become acute, workplaces can use short and focused pulse surveys. Issuing such surveys after reorganizations, layoffs, leadership transitions, or significant public conflicts would enable organizations to gather early warning data. Anonymous feedback channels should complement surveys to capture early risk signals in teams, shifts, or departments that would otherwise be invisible to corporate leadership.

7. Plan for the post-termination window.

Former employees committed a substantially larger share of active shooter cases than of insider homicides overall (33.1 percent versus 20.8 percent). In addition, one in five victims was a supervisor, suggesting deliberate targeting. Supervisors are both the people who deliver reprimands and the people whose decisions most directly shape an employee's economic life. They need more training, better protocols, and structured support for these difficult conversations and situations.

The weeks and months after termination carry elevated risk, particularly for the employees and supervisors most directly associated with the decision. Post-termination monitoring does not require invasive surveillance, but it does require knowing who the high-risk departures are, ensuring that badges and system access are fully revoked, noting concerning post-separation communication, and keeping the workplace threat assessment team involved until the window closes.

Reference

Jillian Peterson and James Densley, *Workplace Homicides*, Violence Prevention Project, 2026, <https://www.theviolenceproject.org/databases/workplace>.

Jillian Peterson and James Densley are cofounders of the Violence Prevention Project, a nonpartisan, nonprofit research center located at Hamline University in Saint Paul, Minnesota.

About CNA

The CNA Corporation (CNA) is a not-for-profit analytical organization dedicated to the safety and security of the nation. Nearly 700 CNA scientists, analysts, and professionals provide data-driven, innovative solutions to complex problems. It operates the Center for Naval Analyses—the Department of the Navy’s federally funded research and development center (FFRDC)—as well as the Institute for Public Research, which supports federal, state, and local government officials advancing national and homeland security.

To learn more about the DVERT Center, contact our team at dvert@cna.org.

Any copyright in this work is subject to the Government’s Unlimited Rights license. The reproduction of this work for commercial purposes is strictly prohibited. Nongovernmental users may copy and distribute this document noncommercially, in any medium, provided that the copyright notice is reproduced in all copies. Nongovernmental users may not use technical measures to obstruct or control the reading or further copying of the copies they make or distribute. Nongovernmental users may not accept compensation of any manner in exchange for copies. All other rights reserved. This report may contain hyperlinks to websites and servers maintained by third parties. CNA does not control, evaluate, endorse, or guarantee content found in those sites. We do not assume any responsibility or liability for the actions, products, services, and content of those sites or the parties that operate them.

CNA® is a registered trademark of The CNA Corporation and may not be used without prior written authorization.