BTAC BULLETIN

BEHAVIORAL SCIENCE | LAW ENFORCEMENT & COUNTERINTELLIGENCE | CYBERSECURITY I EMPLOYEE LABOR RELATIONS I THREAT ASSESSMENT & MANAGEMENT

STALKING

AN INSIDIOUS INSIDER THREAT

Stalking involves a persistent pattern of repeated and unwanted attention, surveillance, and/or harassment that causes fear or distress in those targeted. When these behaviors manifest within an organization, it can compromise security, erode trust, and disrupt operations. Of particular concern is the significant risk of stalking behavior to escalate to violence without appropriate action. However, the subtle intensifying behaviors can be challenging to identify, as it can take many forms and may not always be obvious. Signs of stalking behavior can range from unwanted gift-giving to invasive monitoring of digital communications, or physical surveillance, resulting in constant wariness and anxiety for the victim(s). By acknowledging this risk, and addressing it before it spirals, organizations can foster a safer workplace and decrease insider threats.

1:3

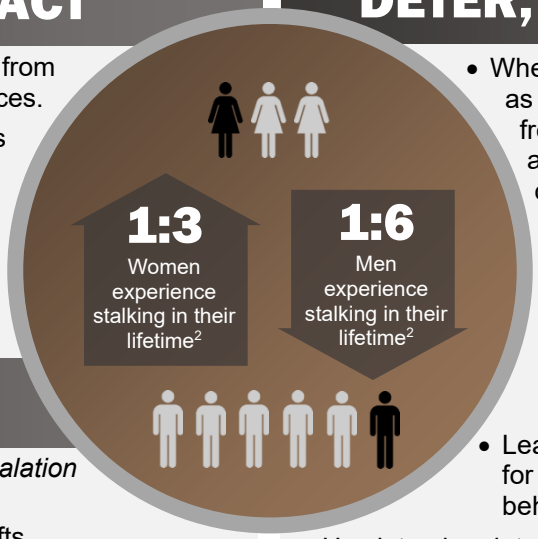
In a 2023 USSS report[1], 36% of mass shooters exhibited stalking/harassment behavior prior to the attack.

WORKPLACE IMPACT

Psychological Toll: Victims often suffer from anxiety, depression, and sleep disturbances.

Workplace Disruption: Stalking disrupts productivity, strains relationships, and creates a hostile work environment.

Security Vulnerabilities: Stalkers may exploit their access to sensitive information or systems to surveil or gain access to their victims.



RISK FACTORS

Risk factors for continued stalking or escalation of stalking behavior to violence.[3]

Gifts/Letters: Presence of unsolicited gifts, materials, or letters.

Previous Relationships: *Victim is a* former intimate partner. *However, up to 41% of stalking victims are acquaintances*[1].

Property Damage: Presence of damage to personal property of the victim.

Criminality/Violence: History of violent or criminal behavior, especially prior domestic violence towards the current victim or others.

DETER, DETECT, MITIGATE

- When reporting stalking behavior document as much detail as possible; nature, frequency, and duration of the behavior and any evidence or witnesses that may corroborate the behavior.
  - Keep a record/log including dates, times, and any correspondence or other evidence, even if it seems minor.
  - Employers may need to adjust workspaces, change schedules, or provide additional security measures.
- Leaders should monitor network traffic (UAM) for suspicious patterns or inappropriate behavior in response to concerns.
- Use intrusion detection systems to identify unauthorized access, to systems, files, or records with no need to know.
- Train employees and managers to recognize signs of both cyberstalking and traditional stalking and encourage the positive bystander effect of “see something say something”.
- Develop clear policies that address both cyberstalking and physical stalking, unauthorized access, and misuse of company resources.

REFERENCES: 1. U.S. Secret Service: National Threat Assessment Center. (2023). *Mass Attacks in Public Spaces 2016-2020.* US Department of Homeland Security.

2. Smith, S.G., Basile, K.C., & Kresnow, M. (2022). The National Intimate Partner and Sexual Violence Survey (NISVS):2016/2017 Report on Stalking. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease control and Prevention 3. McEwan, T., (2021). Stalking Threat and Risk Assessment. In J. R. Meloy & J. Hoffmann (Eds.), International handbook of threat assessment (2nd ed., pp. 210-234). Oxford University Press.