How to Run Effective Workplace Violence Investigations

With the right processes in place, corporate security teams can establish a comprehensive program to address violence and concerning behavior in the workplace. This empowers teams to recognize risk factors, triage, streamline investigations, take proactive measures, and create consistent, compliant incident reports with recommended actions to address concerns and support ongoing analysis.

Leverage the following checklist to ensure you have a comprehensive investigative process in place.

Set Up In Advance

Establish systems and processes

Ensure teams have the right tools in place to proactively monitor for behaviors of concern and establish processes to identify concerns, gather relevant information, assess the concern, mitigate risks, manage/intervene the person of concern, and create standardization in an investigation workflow across the team.

Define who/what needs protection Executives, employees, customers, visitors, office buildings, parking lots, travel, residence	☐
Consolidate connected systems data Vehicle, visitor management systems (VMS), access control, CRM, case management (past and current)	☐
Centralize research and monitoring tools Criminal, civil records, OSINT, social media, dark web, local news reports, localized crime data	☐
Review and update policies to support gathering and storing of information and intervention	☐
Define policies for lone, remote, hybrid, and office work sites	☐
Define triage processes for how initial information is handled/screened	☐
Identify reporting sources Grievances (internal and external), lawsuits, terminations, policy violations, disengaged employees, or reported disruptive, threatening, or concerning behavior	☐
Set up notification flows based on incident type or urgency Corporate security, HR, legal, third-party experts, PR, police, or EHS	☐
Clarify who has the authority to read, write, share, or close a report	☐

Continued on next page

TIP: Sensitive data should be limited to those who have a true need-to-know, like executive protection and insider threats teams, unless certain at-risk conditions are met.

Select conditions for report status or closure and length of storage Inactive, referred to police, threat mitigated, unresolved (most report closures will be 'soft' based on the information at the time of closure)	☐
Update policy/procedures for emergency situations	☐
Provide training to all stakeholders about how and where to report concerns	☐

Monitor and identify potential concerns

By establishing situational awareness based on systems and tools, teams can monitor data sources for pre-incident indicators and/or behaviors of concern.

Continuously monitor connected systems for sources of threatening or concerning behavior Localized crime trends, activist group activity, executive name searches, social media activity, updates to historical cases that trigger a pattern alert	☐
Monitor unusual alerts from connected systems License plate recognition, access controls, visitor management check-ins, HR reports	☐
Review alerts from adjacent systems Intrusion detection, endpoint protection, cyber threat intelligence, fraud detection	☐
Identify early indicators of violence or behaviors of concern Grievances (internal, external), direct employee or guard observation, connected system alerts, reports (HR, supervisors, co-workers), casing/surveillance, observed tailgating, outside sources (family, police)	☐

In the case of an imminent threat, follow internal policy and scripted dialogue for contacting police, then notify appropriate stakeholders.

Intake and Investigation

Identify the person of interest (POI)

With the aid of the established systems and processes, teams can quickly capture and identify behaviors of concern.

Capture the basic who, what, when, and where details What is the concern, how was it identified, who is the victim/target/complainant, who is the POI, along with the when and where, if known	☐
Screen the concern and determine if it meets the team threshold for investigation	☐
Assign lead investigator and initiate investigation workflow	☐

Continued on next page

Gather information about the reported concern and make an assessment

Leveraging a consolidated platform for investigation, documentation, and collaboration, teams can accelerate detailed investigations to scope and document the concern.

If available, utilize the Ontic Threat Assessment Management and/or WAVR-21 workflow to conduct a threat assessment to determine if the person of concern is on a pathway to violence	☐
Collect supporting information to identify a POI and examine their history, current concerning behavior, and any other information that could be beneficial for the team to know and understand Prior performance history, criminal history, civil judgments (if authorized and legal), social media, dark web, local and third-party surveillance footage (e.g. building security), email, text, or audio information	☐
Collect relevant information from individuals to understand the concern, the timeline in which it occurred, who was impacted, and what parts of the business were disrupted, if any Interview the person who reported the incident, the potential victim(s)/target(s), manager of the victim and/or POI, or co-workers/others who may have information	☐
Collect supporting information from community/outside sources Law enforcement, mental health, community stakeholders	☐
Interview the POI (conducted by HR, legal, security, or police)	☐
Analyze previously documented incidents, investigations, or crime data to determine if there are any connections or related concerns	☐
Document all information gathered in a central platform	☐
Make the assessment – based on the information gathered and known at this time, does the person of concern pose a threat to themselves, others, or both?	☐
If your team uses a priority level to manage, determine priority level based on threat assessment	☐

Built into the Ontic Platform, the Ontic Threat Assessment Management and WAVR-21 workflows help teams organize and analyze the information gathered to determine if someone is on a path to harm. These workflows add fidelity to your inquiry by showing that each concern is treated equally.

Manage the person/situation and reassess regularly

If a pathway to harm (self, others, or both) is identified, implement mitigation strategies	☐
Take any appropriate management actions based on security, HR, and risk management input to contain or mitigate the threat Explore intervention/management strategies available internally and externally	☐
Notify leadership team and expand notifications as needed Building security, media relations, internal communications, any parties who need to know	☐
Document management strategies taken	☐
Regularly review, reassess, and update assessment and management strategies as needed	☐

When a case closes, always caveat it “based on the information available at this time.” Should new information become available, the team should reopen or continue the investigation.

Post Investigation

Analyze data, metrics and trends

Teams with robust metrics and dashboards can analyze trends and data to inform preparation and response activities, preserve knowledge, and evolve investigation best practices.

Track investigation data across a wide variety of variables Case disposition status, case resolution rate, incident type, personnel, location	☐
Build custom reports against any collected data field or emerging threat signal to gain investigation insights	☐
Define document retention period to ensure you're legally compliant and to guard against re-emergence of issues	☐
Conduct an after-action review What happened, what was learned, what can be done to improve	☐
Set up evaluation dates Trigger a threat review on significant dates (e.g. event anniversary)	☐