Workplace violence (WPV) cannot be 100% prevented. However, we know from experience that well-placed preparedness and prevention measures can significantly diminish the probability and severity of potential workplace violence.
A prime example comes as an outgrowth of the multiple “going Postal” shootings at the U.S. Postal Service (USPS) by employees or ex-employees (mostly in the 1990s). Out of necessity, USPS implemented a comprehensive workplace violence programme throughout their organisation. As a result, with approximately 750,000 employees at the time, USPS went over eight (8) years without an employee or ex-employee shooting by utilising a workplace violence programme like the programme outlined herein. This author contributed to the development and implementation of the USPS programme in the 1990s.

**Formal people management training**

One noteworthy component that was implemented appeared to be a major contributor to the success of the USPS programme. Previously, supervisors and managers were promoted from within the ranks with no formal training in “people management.” The culture was one of mostly autocratic, top down management. As a part of the WPV programme, supervisors and managers were trained not only in identifying and reporting WPV threatening situations, but also in how to lead with dignity and compassion. The latter component seemed to be a vital cultural component that led to the success of the WPV programme.

**How to design a Workplace Violence Programme**

The following components of a comprehensive Workplace Violence Programme can be used as a template to assess one’s present WPV programme. This exhaustive list includes all the main components, and may include more or fewer controls according to individual organisation’s culture.

**Workplace violence policy:** Defines workplace violence and consequences for policy

Contains verbiage that will support managers who must confront potentially violent individuals. Content is periodically updated to address new issues and State laws, e.g., concealed weapons, gun possession in vehicles at work, bullying, discrimination, etc. Some organisations omit the “zero tolerance” statement in belief that it inhibits reporting of
violations by employees who erroneously believe it implies automatic firing of violators.

**Threat notification system:** Clearly communicated availability and access for reporting threatening behaviour and situations. Confidentiality for those who report is addressed. Anonymous reporting is typically available. Disciplinary action is defined for those knowingly making false reports. Reporting can be provided through an internal vs. external provider. Ongoing reminders (posters, flyers, etc.) are provided to employees and supervisors.

**Social media intelligence monitoring:** Ongoing monitoring of openly available social media posts that identify warnings, threatening discourse, mental health disorders associated with violent ideation, and other signs of violence against people and the workplace. Monitoring can be provided through internal or external resources. Protocol is established for reporting monitored threats to management and timely, appropriate response.

**Threat management team:** Multidisciplinary management team trained and exercised in handling threatening situations. The team is responsive to threat notifications on a timely and thorough basis. At a minimum, representation from legal, HR and security are core members. Other disciplines are included, e.g., union reps and/or additional staff positions, as appropriate. External team members and specialists are included as core or ad hoc members.

**External relationships established:** Relationships are established with professionals and specialists to support the Threat Management Team, e.g., local law enforcement, threat assessment and defusing professionals, attorney(s), judges with jurisdiction over domestic violence and injunctive relief, guard services, surveillance, covert, investigations, executive protection, dispute resolution, hostility management, linguistic analysis, IT forensics, polygraph testing, outplacement services, etc.

**Threat management team manual and system:** Clear and actionable guidelines for
managing threatening situations are utilised for effective, efficient and defensible threat management. The same protocol is used, even though team members may change. Guidelines include immediate actions, assessment, investigations, defusing methods, follow-up, purposeful disengagement, and legally compliant documentation. Authority, communications and expectations are defined.

**Pre-employment reference checking / Criminal background checks:** Reference-check questions to assess potentially violent job applicants that previous employers feel compelled to report, e.g., “So I can document my file, do we have any reason to be concerned about this applicant from a workplace violence standpoint?” Protocol for legally-compliant pre-employment and “for-cause” criminal background checks.

**Character-based pre-employment interview questions:** Pre-employment interviews designed to identify individuals with violent history, character problems, entitlement issues, anger and sociopathic tendencies. Compliance with “ban the box” legislation related to hiring persons with criminal histories.

**Hostility management training:** Take-and-use methods for managers, supervisors and employees regarding how to calm hostile situations in real time vs. Inadvertently provoking increased aggression or violence.

**Corporate security programme:** Physical and IT Security Director(s) that integrate violence-related threat management (prevention, preparedness and response) with other appropriate corporate disciplines, e.g., HR, legal, facilities, site management, unions, etc. Methods established for investigating electronically-generated threats.

**Physical security audit:** Periodic assessment of facilities, property, security systems and other methods for monitoring and preventing breaches and potential violence. It is best if this audit is conducted under attorney privilege.

**Tracking of threatening situations:** Ongoing Management Information System (MIS) that identifies, compiles, and tracks data re: the occurrences of threats (toward people, the organisation, reputation, and/or property) i.e., electronic, written, verbal, symbolic, etc. Risks may be related to location of workplace(s) in a community, industry incidents, local crime
rates, employee population, previous incidents, near misses, etc. Tracking of motives could be related to supervisor/employee conflicts, employee-on-employee hostilities, domestic violence, drugs and alcohol, crime/robberies, toxic work environment, union/management conflicts, activist groups, terrorism, political, kidnap and ransom, etc.

**External provider screening:** Investigation of methods used by external providers to screen out potentially violent contractors in your workplace, e.g., temporary placement agencies, catering services, consultants, contractors, security services, etc.

The WPV programme should include reference-check questions to assess potentially violent job applicants that previous employers feel compelled to report.

**Layoffs/Terminations protocol:** Guidelines and protocol for preparation and implementation of disciplinary meetings, layoffs, and for-cause terminations when hostility and potential violence are a concern. Caring communications, crisis actions, staging of the meeting, law enforcement or guard services, threat assessment and defusing psychologist, outplacement services, severance payments, protection of dignity, etc. may be included in the preparedness planning.

**Supervisory training:** Methods for disciplining and managing employees who are
potentially violent or hostile. Skills training regarding the people-side of supervision, e.g.,
caring and compassionate handling of employee issues and human complexities that arise
during supervision and working relationships.

Employee workplace violence publicity: Ongoing information about the organisation’s
WPV programme, recognising and reporting threatening situations, and hostility
management methods. Orientation for employees at least annually and for new employees.

Employee assistance programme: EAP provider that has access to skilled anger
management specialists and an internal threat-related “duty-to-warn” protocol that involves
more than solitary judgment of the clinician, i.e., collaborative/supervisory procedures when
potential violence is a concern. EAP professionals that are trained in boundary issues
regarding when it's appropriate to utilise outside resources into potentially violent situations,
e.g., organisation’s management, law enforcement, threat specialists, etc. Avoidance of
unethical “dual relationships” where the EAP is serving the threatening individual and the
Threat Management Team simultaneously. EAP should have local domestic violence
relationships, e.g., women’s shelters, men’s stopping violence groups, etc.

Domestic violence programme: Guidelines and assistance for employees who are
subjected to, or notice evidence of, domestic violence. Protocol for domestic threats that can
come into the workplace, if additional employees are targeted, and when restraining orders
are issued by employees, especially when the violator’s access to the workplace is
prohibited.

Employee survey: Inclusion of violence issues in employee surveys.

Alternative dispute resolution programme: Methods to address situations that may
include hostilities and potential violence, e.g., structured intervention by threat-experienced
psychologist, coaching, facilitated communications, negotiation, mediation, collaborative law
and arbitration.

Emergency and post-crisis response system: Evacuation, shelter in place, active shooter
plan, lock down, safe rooms, etc. with employee/supervisory training and exercises on a
periodic basis. Floor warden system. Beyond emergency response, development of strategic crisis management preparations for senior management to protect core assets affected by violent incidents, e.g., employees, key relationships, reputation, finances, shareholder value, brand, operations and physical/intellectual property.

These guidelines are listed as a generic template to help an organisation evaluate their present Workplace Violence Programme. A comprehensive programme may not include each of these components and it may include other elements that are not listed herein. This checklist is to be used with prudent management judgment in designing a comprehensive Workplace Violence Programme that best fits the organisation’s time, budget, culture, and risk tolerance.

Author Profile

Bruce Blythe
You may also be interested in...

Creating a safe and secure workplace environment using a culture of openness

Companies that have developed a culture of openness can provide and receive feedback at all levels. The nail that sticks...

Workplace violence is declining, but employers still need guidance

While the number of incidents is falling, hundreds of thousands of workplace violence incidents still occur every year. More...

Detecting workplace violence with sound detection and audio analytics

Workplace violence has been on the rise in mental health facilities, schools, and detention centres across the country. According to the Occ...