Considering the dynamics of human behavior, Threat Management requires a team. In particular, one that is multidisciplinary in composition. The ASIS International *Workplace Violence and Active Assailant--Prevention, Intervention and Response Standard* (ANSI/ASIS WVPI AA-2020 Standard) outlines:

> "A WVPI program should include a multidisciplinary team created and periodically trained to evaluate and respond to violent incidents or reports of concerning behavior made. Creating and training a Threat Management Team helps to ensure that lines of authority and communication and a general incident management process are established before a threat or violent incident occurs, and that personnel will know how to respond to reports concerning workplace violence."

Federal OSHA also recognizes the importance of having a Threat Management team. While using different language, a TMT is a quality means to align with OSHA guidance, as outlined:

> "Provide management support during emergencies. Respond promptly to all complaints. Set up a trained response team to respond to emergencies. Use properly trained security officers to deal with aggressive behavior. Follow written security procedures... Employee assistance programs, human resource professionals and local mental health and emergency service personnel should be contacted for input in developing these strategies."

Commonly, personnel that staff the TMT are also responsible for managing the overall WVPI program. There are multiple ways to establish this team, which is largely dependent on organization size, geographic placement, organizational culture, and other factors. Check out the section below on *Threat Management Team Models* to learn more.

Creating an effective TMT requires the integration of diverse expertise from various departments within the organization. This multidisciplinary approach ensures that the team can comprehensively assess, manage, and respond to potential threats. While TMT composition will vary by organization, the following functions formulate a typical TMT. It's important that the TMT includes members that represent the totality of the organization to maximize understanding and insights when cases arise. A TMT should also have *primary* and *alternate* positions filled for the core team, while other positions may only be needed on an ad hoc basis.

Core Functions for a Threat Management Team

- Security - Provides insights into potential vulnerabilities, coordinates incident response, and implements preventive measures. Commonly, Security personnel manage TMT operations day-to-day.
- Human Resources - Manages employee relations and ensures that workplace policies are enforced. They handle reports of concerning behavior and provide support for affected employees.
- Legal - Ensures all actions taken by the TMT comply with relevant laws and regulations. They provide guidance on legal implications and help mitigate liability risks.

Other Potential Members

- Communications - Handles internal and external messaging during a threat or incident. They ensure that information is disseminated accurately and efficiently.
- Collective Bargaining Representatives - Advocates for the rights and safety of unionized employees. They work with the TMT to ensure that measures respect union agreements and support employee welfare. Union inclusion, when relevant, is important for BTAM effectiveness.
- Employee Assistance Program (EAP) - Offers confidential support services to employees dealing with personal or work-related issues that could impact their behavior. While EAP personnel may not be able to share information with the TMT, the TMT may share information with the EAP, which can help improve prevention strategies.
- Facilities Management - Oftentimes, ensures that the physical work environment is safe, secure, and operating effectively. They collaborate with the security team to manage access control and safety infrastructure and can help prevent unauthorized access.
- Risk Management - Assesses potential risks and develops strategies to mitigate them, helping members of the TMT identify and address vulnerabilities. Risk Management may also oversee insurance for the organization, which might be applicable to incidents that arise, such as Workers Compensation issues.

- Information Technology and/or Cybersecurity - Identifies behavior that may be present on organizational information systems, authorizes and/or prohibits access to systems, and can share applicable information with the TMT.

Need help composing your team? We're here to help—reach out any time!