Safeguarding Your Corporate Leaders Against Rising Security Threats: FP's Guide on Executive Protection

Insights
4.25.25

Today's corporate leaders face a wide range of potential security threats, and recent high-profile incidents have brought that vulnerability into sharp focus. Executives are increasingly at risk of becoming targets of violent acts or cyberattacks such as doxing or social engineering, and your organization must think ten steps ahead to ensure the safety of your people and the future of your business. To wrap up Workplace Violence Prevention Awareness Month, we'll give you an overview of executive protection programs and four key steps to get you started.

Executive Protection is One Piece of Workplace Violence Prevention

April is Workplace Violence Prevention Awareness Month, and employers should use this as an opportunity to learn more about workplace violence issues and how to address them. Earlier this month, we covered why employers must take workplace violence prevention seriously and compiled 10 strategies that can help protect your employees and your organization. For a deeper dive, check out FP's Workplace Violence Prevention Awareness Kit for Employers.

This insight focuses on executive protection – an important but distinct type of workplace violence prevention. While some aspects of executive protection may implicate employer obligations under federal and state laws applicable to recognized workplace violence hazards, other aspects may fall outside of that umbrella or implicate other obligations.

To start, here's what execution protection means – according to security professionals.

- **Executive protection (EP)** includes "the practices, strategies, and technologies used to safeguard high-profile individuals, including CEOs, government officials, and other executives, from physical harm and other threats, " according to one threat intelligence provider.
- **EP agents** approach risk much differently than bodyguards, says Mena Ghali, the CEO of a private security services provider. According to Ghali, while bodyguards are "reactive powerhouses stepping up when things get physical," EP agents operate "like a chess master playing several moves ahead" and avoid danger "by mastering protective intelligence and strategic planning skills."
- **Effective EP programs** must be "thoughtfully designed and horizontally integrated with other security functions, including intelligence, physical security, cyber security, and crisis management, supported by clear policies, procedures, and training," writes Rick Mercuri, a corporate security advisor with decades of experience.

Why Your Organization Should Consider Implementing an EP Program

An EP program protects not only the safety and well-being of your corporate leaders but also your business. For example, a sudden leadership vacuum or a violent incident involving a company executive can disrupt your organization's operations, decrease productivity, cause reputational harm, and create legal exposure.

- **The Legal Landscape.** As mentioned above, federal and state safety laws require employers, at least to some degree, to protect their executives from violence hazards at work – such as under the general duty clause of the federal Occupational Safety and Health Act (OSH Act). In addition, several states have laws or regulations requiring employers in specific industries such as healthcare or retail to develop workplace violence prevention plans. In contrast, California requires virtually all employers to develop and implement workplace violence prevention plans. These workplace violence laws are expected to become increasingly more common as bills are introduced in state legislatures throughout the country.
- While some aspects of executive protection may be outside the scope of such laws (such as providing personal security to leadership and their family members outside the workplace), corporate directors and officers may potentially have fiduciary duties (such as the duty of oversight) to provide protect their corporate leaders.
- **Rising Threats.** The New York Times reported in December that targeted attacks against executives have risen over the past five years, "partly because digital platforms have made it easier to obtain information about identities and locations, and social media has fanned the flames of vitriol." The NYT article also states that the "median amount spent on executive security among the S&P 500 companies that disclose such information doubled from 2021 to 2023."

Establishing an EP program is even more critical if your organization faces increased risks due to your industry (for example, the healthcare, retail, technology, and hospitality industries each present unique and heightened vulnerabilities), your executives' visibility, or the current political climate.

Key Features of Effective EP Programs + 4 Steps You Can Take Now to Get Started

Executive protection is no longer limited to celebrities or dignitaries, and it is more than just a C-suite luxury. Unfortunately, rising threat levels make EP programs a business necessity for many larger companies.

A modern EP program should be:

- **tailored** to the unique risks each corporate leader faces;
- **multidisciplinary**, blending cybersecurity, threat intelligence, secure transportation planning, real-time monitoring, and emergency protocols; and
- **adaptable and regularly updated** to address different scenarios and fluctuating risk levels.

Here are four steps you can take now to start building an effective EP program:

1. **Establish operating procedures and a multidisciplinary team.** Your executive protection program should be guided by clear protocols that are carried out by a multidisciplinary team of diverse professionals, such as physical security, cybersecurity, and threat intelligence specialists, as well as HR leaders, crisis managers, travel risk management experts, and legal counsel. Your EP strategy should take a proactive approach but also address emergency response protocols, crisis communications, and other critical reactive measures.
2. **Conduct individualized threat assessments.** Members of your multidisciplinary team should evaluate all potential threats facing a particular executive and consider specific risk factors, such as the executive's participation in public events or polarizing business decisions to their travel habits, family circumstances, and personal history. Remember that threats may arise from disgruntled and recently fired employees or from individuals or groups who have never worked for your organization, such as political activists, angry customers or patients, or cybercriminals.
3. **Develop (and regularly update) tailored security plans**. Based on individualized threat assessments (and continuous threat monitoring), you should create personalized and highly detailed EP strategies for each executive that can help mitigate the unique risks they face both on a regular basis and in various specific scenarios. Your plan will need to allocate resources appropriately, utilize advanced security technologies, and equip your executives and their teams with the knowledge, skills, and tools to respond to threats effectively.
4. **Prepare a crisis communications plan.** When a crisis erupts at your organization, you won't have time to develop a response from scratch. Instead, you'll need to have a robust crisis communications plan already in place so you can effectively communicate with your employees, stakeholders, customers, and the general public. To learn more, check out our 10-Step Crisis

Communications Playbook for Employers or reach out to any member of our Crisis Communications and Strategy Team.

Conclusion

We will monitor developments in this area and provide updates as warranted. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have any questions, contact the authors of this Insight, your Fisher Phillips attorney, or any member of our Workplace Safety Team or our Crisis Communications and Strategy Team.

Related People

Rick Grimaldi
Partner
610.230.2136
Email

Andrew J. Sommer
Partner
213.330.4487
Email

Hannah Sweiss
Partner
818.230.4255
Email

Kristin R.B. White
Partner
303.218.3658
Email

Service Focus

Counseling and Advice

Crisis Communications and Strategy

Workplace Safety and Catastrophe Management

Industry Focus

Healthcare

Hospitality

Retail

Tech