ZEROFOX

WHITE PAPER

Executive Protection Plan Framework

Protect your leaders with a modern, actionable blueprint for today's evolving threat landscape.



INTRODUCTION

Executive Protection Planning in 2025

Your CEO's online footprint is bigger than you might think. And it's not just their personal LinkedIn. It's leaked itineraries. Their kids' Instagram stories. A news photo that quietly geotags their home.

In 2025, the most serious threats to high-profile executives often start online—before anyone realizes they've crossed into the real world. A leaked credential becomes an account takeover. A deepfake opens the door to extortion. A disgruntled ex-employee finds a phone number on a data broker site and shows up at the front door.

Traditional security teams weren't built for this. They watch and protect the physical world. But today's attackers often start behind a screen.

This guide introduces the Executive Protection Plan Framework—a strategic blueprint for modern protection. It blends digital risk protection with geospatial intelligence and real-time monitoring to help organizations spot the earliest signs of threat and stop escalation before it happens.

60%
of VIPs have data for sale on underground marketplaces

75%
of leaders have experienced credential exposure

105K
Physical Security Alerts validated by ZeroFox in 2024

Table of Contents

Why Risk Follows Executives Everywhere 1

Building A Strong Executive Security Plan 2

Risk Assessment Checklist 3

Sample Plan Framework 4

ZeroFox for Executive Protection 7

About ZeroFox 8

©2025 ZeroFox Inc. All rights reserved. All other trademarks are property of their respective owners.

Why Risk Follows Executives Everywhere

The executive threat landscape has shifted dramatically in the past decade. What was once the domain of stalkers and fringe threats has evolved into a complex web of digital and physical risks, many of them interconnected. Today's executives are high-visibility symbols of corporate values, policies, and stances, making them lightning rods for a wide range of adversaries, from cybercriminals and activists to disgruntled insiders and sometimes even nation-states.

Executives today are thought leaders. They're expected to maintain a visible, vocal presence on social media, at public events, and in the news. But that visibility comes with risk. Personal lives are exposed online. Children may unknowingly share sensitive details on social platforms. Executive travel plans can be uncovered through public posts or leaked itineraries. Even seemingly unrelated controversies, like a corporate restructuring or a politically charged environmental policy, can escalate to targeted harassment campaigns or real-world incidents.

Add to these issues the rising number of insider threats, workplace violence incidents, and geopolitical tensions and it's clear why executive protection can no longer rely on physical surveillance alone. Traditional security measures don't cover what threat actors can do and see online.

Typically, executive threats fall into four core categories, all of which must be addressed in a modern protection program:

- **DIGITAL THREATS** include credential theft, impersonation scams, and account takeovers. With the rise of generative AI, deepfakes, and real-time phishing tactics, attacks are more convincing—and more damaging—than ever.
- **PRIVACY CONCERNS** are fueled by rampant PII exposure, with executive data like home addresses and phone numbers often sold on dark web forums or harvested from data broker sites.
- **REPUTATIONAL RISKS** emerge from fake profiles, misinformation campaigns, and fraudulent partnerships—many of which start with a single impersonation and ripple out to impact customers, investors, and the brand at large.
- **PHYSICAL THREATS** range from nuisance-level harassment to real-world violence, including harassment on the street, home invasions, and kidnapping attempts.

In 2025, the most dangerous threats often begin as digital breadcrumbs that can evolve into physical danger if left unchecked. ***The modern threat landscape demands a proactive, integrated approach that fuses digital risk protection with physical security intelligence,*** tailored to the unique risk profile of every executive.

©2025 ZeroFox Inc. All rights reserved. All other trademarks are property of their respective owners.

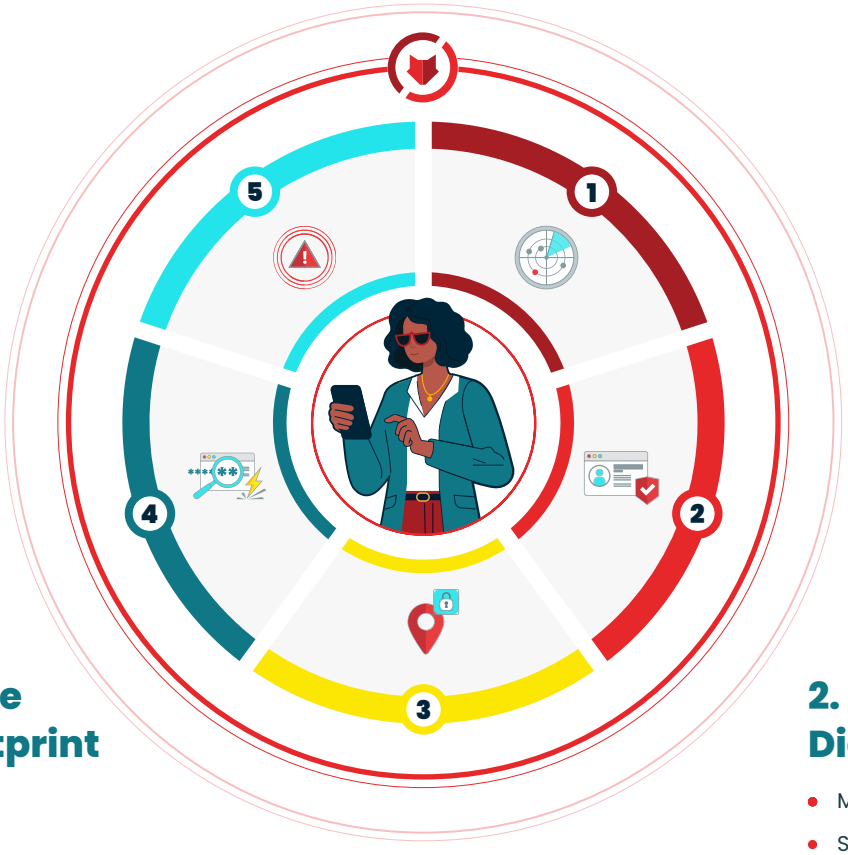
Building A Strong Executive Security Plan

5 Key Pieces to Your Executive Security Plan

In our converging digital and physical world, it's up to organizations to help keep leaders safe. Here's what you should include in your organization's executive security plan.

5. Real-time notifications

- Pre-travel risk assessments
- Monitor threats in real time during travel
- Coordinate secure transportation & lodging
- Plan for emergency response



1. Map the Risk with Intel

- Evaluate public profile & visibility
- Analyze industry-specific risks
- Identify active threat actors
- Track historical & emerging threat patterns

4. Guard the Digital Footprint

- Remove PII from data broker sites
- Monitor leaked credentials
- Lock down personal & family info
- Extend privacy training to loved ones

3. Safeguard the Physical World

- Get real-time alerts for physical threats
- Address stalking, harassment & protests
- Respond to unrest or violence
- Customize protection based on risk (travel, events, 24/7)

2. Defend the Digital Front

- Monitor for impersonations
- Scan deep & dark web for attack chatter
- Secure social accounts
- Automate takedowns of fake profiles
- Gather & analyze digital threat intel

©2025 ZeroFox Inc. All rights reserved. All other trademarks are property of their respective owners.

Risk Assessment Checklist

Building an effective executive protection plan starts with a comprehensive risk assessment. Here's a step-by-step approach:

STEP 1: Decide Who Needs Protection

CHECKLIST TRACKER

Identify the individuals most at risk:

- [ ] C-suite executives and board members
- [ ] High-profile or public-facing employees
- [ ] Team members with access to sensitive data (such as Finance, Legal, IT, and HR)
- [ ] Immediate family members of protected individuals

STEP 2: Use Automation & AI for Vulnerability Detection

CHECKLIST TRACKER

Deploy smart tech to uncover risk faster:

- [ ] AI-powered monitoring of social media and public platforms
- [ ] Automated alerts for credential exposure and data leaks
- [ ] Image recognition tools to flag impersonations
- [ ] NLP (Natural Language Processing) to detect threatening or harmful content

STEP 3: Extend Visibility with Human Intelligence

CHECKLIST TRACKER

Pair automation with expert analysis:

- [ ] Analyst validation of high-priority alerts
- [ ] Threat researchers to track trends and attacker behaviors
- [ ] Intelligence professionals to add context and nuance
- [ ] Engagement specialists for threat actor interaction, if needed

STEP 4: Take Proactive Risk Reduction Measures

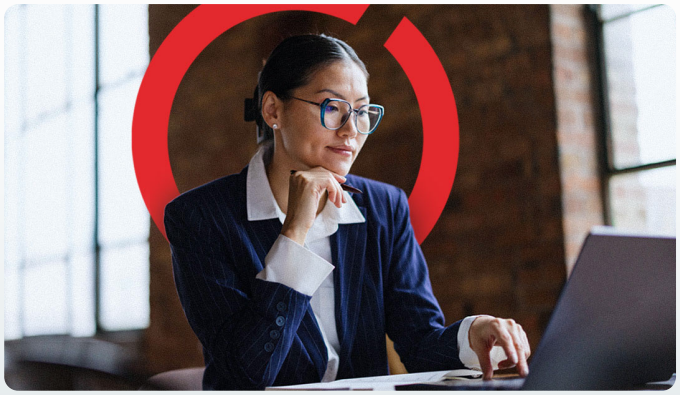
CHECKLIST TRACKER

Manage your attack surface before threat actors strike:

- [ ] Ongoing removal of exposed PII from data broker sites
- [ ] Hardened privacy settings on personal and professional accounts
- [ ] Secure travel protocols and destination risk assessments
- [ ] Awareness training for executives and their families

©2025 ZeroFox Inc. All rights reserved. All other trademarks are property of their respective owners.

Sample Plan Framework



When it comes to executive safety, it's clear that ad hoc security won't cut it. Threat actors today exploit every possible vulnerability, from physical gaps in event security to impersonations spreading online in seconds. A strong executive protection plan anticipates these threats. That means combining real-time intelligence, physical protection, and digital risk mitigation into one unified strategy. Below, we break down an executive protection framework covering both physical and digital planning.

Physical Executive Protection Planning

Physical threats have evolved. To meet them head-on, your plan needs to go beyond security guards and cameras. Here's how to structure physical protection that adapts with your executive's movements, public exposure, and personal risk profile.

CORE PROTECTION TEAM STRUCTURE

Build a multidisciplinary team:

- **Executive Protection Manager:** Oversees the entire program
- **Close Protection Agents:** Provide direct physical security
- **Intelligence Analysts:** Monitor threats and provide situational awareness
- **Technical Security Specialists:** Handle electronic surveillance and countermeasures
- **Residential Security Officers:** Secure the executive's home and property

INTELLIGENCE COLLECTION & DISSEMINATION

Keep your team informed with:

- **Daily intelligence briefings** for the protection team
- **Regular executive threat assessments** using multiple intelligence sources
- **Secure communication channels** for distributing sensitive intelligence
- **Structured reporting protocols** with clear escalation pathways
- **Integration of real-time intelligence** feeds with physical security operations
- **Feedback loops** between field teams and intelligence analysts

ADVANCE PLANNING FOR TRAVEL & EVENTS

Prevention starts with preparation:

- **Pre-trip intelligence** gathering and risk assessment
- **Route planning** and alternative options
- **Venue security** coordination and site surveys
- **Transportation** arrangements and secure vehicle preparation
- **Local resource** identification

PRO TIP:

Don't Skip the Advance Work

Most physical threats can be neutralized before they escalate, with proper planning. Site surveys, alternate routes, and local intel should be mandatory for every event or trip.

©2025 ZeroFox Inc. All rights reserved. All other trademarks are property of their respective owners.

COUNTER-SURVEILLANCE TECHNIQUES

Employ sophisticated methods:

- **Technical surveillance countermeasures** (TSCM) sweeps of vehicles, offices, and residences
- **Detection of surveillance devices** and potential listening equipment
- **Route variation** and randomization of travel patterns
- **Counter-surveillance operators** deployed ahead of executive movements
- **Social media monitoring** for location disclosures and planned disruptions
- **Recognition of surveillance indicators** and anomalous behavior patterns
- Regular training and exercises to maintain counter-surveillance skills

RESIDENTIAL SECURITY BEST PRACTICES

Home should be a safe zone. Security measures should include:

- **Access control systems** and protocols
- **Surveillance cameras** and monitoring
- **Perimeter security** and intrusion detection
- **Panic rooms** or safe zones
- **Emergency response** procedures

REAL-WORLD INSIGHT:

The Home as a Soft Target

Executives often have better security at work than at home. One ZeroFox client uncovered multiple posts on a dark web forum detailing floorplans of an exec's vacation home—PII leaked via a breached real estate app.

Digital Executive Protection Planning

Your executive's biggest exposure isn't on the stage—it's online. Threat actors impersonate, dox, and track executives across social platforms and dark web forums, using leaked data to fuel real-world threats. Digital protection must be just as rigorous as physical security and deeply integrated with it.

IMPERSONATION MONITORING

With social media impersonations on the rise, continuous monitoring is vital. You need capabilities such as:

- **AI-powered image analysis** to detect fake profiles
- **Automated scanning** of social platforms for unauthorized accounts
- **Rapid takedown** procedures for fraudulent profiles
- **Monitoring of emerging platforms** for new impersonation attempts

PII REMOVAL & PRIVACY SHIELDING

To combat executives' personal information being routinely collected and sold by data brokers, you need:

- **Continuous scanning** of hundreds of data broker sites for executive PII
- **Automated removal** requests to eliminate exposed information
- **Ongoing monitoring** to prevent re-listing of removed data
- **Family member protection** to reduce the extended attack surface
- **Regular reporting** on PII exposure and removal effectiveness

REAL-WORLD INSIGHT:

What's for Sale on the Dark Web?

PII, credentials, passport scans, SIM card cloning services—even real-time GPS trackers—are regularly listed. ZeroFox monitors these markets to surface credible threats before they become real-world incidents.

©2025 ZeroFox Inc. All rights reserved. All other trademarks are property of their respective owners.

DARK WEB MONITORING

To ensure that the dark web isn't a breeding ground for threats against executives, you must take steps to:

- **Monitor** for leaked credentials and PII
- **Track** mentions of the executive on underground forums
- **Identify** sale of executive data on illicit marketplaces
- **Analyze** threat actor communications and plans

PRO TIP:

Pair AI with Analyst Eyes

AI catches the volume, humans catch the nuance. The most effective protection strategies rely on this one-two punch to cut through the noise and zero in on real threats.



Integrate Digital Intelligence into Physical Security Operations

The best modern executive protection bridges the digital-physical divide with:

REAL-TIME PHYSICAL SECURITY ALERTS
based on social media activity

MOBILE APPLICATIONS
that provide location-based threat intelligence

AN EARLY WARNING SYSTEM
for planned protests or demonstrations near executive locations

COORDINATION
between digital intelligence analysts and physical security teams

GEOLOCATION TRACKING
during executive travel with threat overlay

©2025 ZeroFox Inc. All rights reserved. All other trademarks are property of their respective owners.

ZeroFox for Executive Protection

ZeroFox safeguards more than 19K high-profile executives, VIPs, and leaders across government, military, and Fortune 1000 organizations. Serving industries from financial services and technology to healthcare and academia, our end-to-end external cybersecurity solution delivers unmatched protection for today's most targeted individuals.

We specialize in identifying and neutralizing threats that originate outside your perimeter—across social media, news platforms, criminal marketplaces, and even the dark web. Whether it's a doxxing attempt, impersonation scam, or physical safety risk, ZeroFox delivers the intelligence and takedown power you need to stay ahead of it.

350K

Successful Executive Impersonation Takedowns in 2024

529K

Physical Security Alerts Generated in 2024

Your Executive Protection Program

ZeroFox tailors your executive protection plan to your organization's unique threat landscape, built on four key capabilities:

AUTOMATED SOCIAL MEDIA MONITORING

Continuously scan the surface web and social media networks, quickly detecting and removing impersonation or malicious content—not just for the executive, but for their immediate family.

DEEP & DARK WEB MONITORING

Dive into the depths of the internet to uncover doxxing, compromised account credentials, and emerging threats.



PII EXPOSURE DISCOVERY AND REMOVAL

Pinpoint and eliminate sensitive personal data leaks for both VIPs and their families, strengthening your overall security posture.

LOCATION-SPECIFIC INTELLIGENCE

Monitor key locations and travel routes, delivering real-time insights to safeguard your high-value protectees wherever they are.

Full-Spectrum Threat Intelligence

In addition to robust tactical alerting, our dedicated intelligence team produces continuous, high-quality global finished intelligence, including:

- Executive Threat Assessments
- Travel & Geopolitical Assessments
- Event Assessments
- Person of Interest Investigations

©2025 ZeroFox Inc. All rights reserved. All other trademarks are property of their respective owners.

ABOUT ZEROFOX

The Leader in External Cybersecurity

ZeroFox is the trusted leader with over a decade of cybersecurity SaaS expertise protecting enterprise digital landscapes—where business operations, customers, and threat actors converge. Through its AI-powered Digital Risk Protection (DRP) solutions, seamlessly integrated with Threat Intelligence (TI) and External Attack Surface Management (EASM) capabilities, ZeroFox empowers organizations to proactively monitor, detect, and disrupt emergent threats by cyber attackers targeting their brands, domains, and people.

Want to see how ZeroFox protects thousands of executives around the world?

Get a closer look at our executive protection platform.

Schedule a call with our team today

See ZeroFox in action

zerofox.com/demo | zerofox.com

Get in touch with us today

sales@zerofox.com | 855.736.1400

©2025 ZeroFox Inc. All rights reserved. All other trademarks are property of their respective owners.