

Executive Security Assessment

Senior leaders are increasingly visible, mobile, and exposed to a wide range of risks, from routine travel disruption to targeted threats and reputational scrutiny. Ensuring their safety, privacy, and freedom to operate requires more than ad-hoc arrangements or reactive measures.

This Executive Security Assessment is designed to help organisations evaluate whether their current approach provides appropriate protection across travel, public activity, and day-to-day operations. It focuses on practical considerations such as oversight, coordination, intelligence support, and response capability - all of which contribute to a resilient, proportionate security posture.

Digital Security

Threat Monitoring

Yes No

→ Are we monitoring for threats against our executives and our organisation on the following sites and platforms?

☐ ☐

a. All social media channels

d. Discord

g. Alt-Social

b. Reddit

e. Telegram

c. 4chan/8chan/8kun

f. Message boards

→ Are we conducting threat monitoring before and during events executives are attending?

☐ ☐

→ Is there a protocol for investigating and responding to potential red flags found online?

☐ ☐

Social Media and Online Presence

→ Are we educating our executives on social media hygiene and best practices around personal privacy?

☐ ☐

→ Is there a policy governing family members' social media use and online presence?

☐ ☐

→ Are we regularly monitoring the digital footprints of our executives and their family members for potential security risks?

☐ ☐

Privacy Protection

→ Could someone find out where our executives live, vacation, and where their kids go to school?

☐ ☐

→ Have we invested in Personally Identifiable Information (PII) deletion services to remove executive information from data brokers and people-search engine websites?

☐ ☐

Physical Security

Residential

Yes No

→ Are the executives' residences equipped with modern security systems, including alarms and CCTV?

☐ ☐

→ Is someone monitoring these alarms and cameras 24/7 and is there a defined response protocol?

☐ ☐

→ Is the system hardwired (instead of being reliant on Wi-Fi)?

☐ ☐

→ Is there a dedicated security team for each primary residence?

☐ ☐

→ Are there regular security audits of residential properties?

☐ ☐

Physical Security (cont.)

Personal Protection

Yes No

- Do executives and family members have access to trained personal protection officers when needed? ☐ ☐
- Is there an established protocol for assessing the need for personal protection during travel or public events? ☐ ☐
- Are the executives' travel patterns varied, making their movements harder to track by malign actors? ☐ ☐
- Is there security on-site during public engagements and appearances by the executives? ☐ ☐
- Are there regular reviews of the executives' close protection program? ☐ ☐

Travel Security

- Is there a process for conducting pre-travel risk assessments? ☐ ☐
- Are we conducting advances ahead of executive travel? ☐ ☐
- Are secure ground transportation arrangements pre-vetted? ☐ ☐
- Is there a system for monitoring the location of executives and family members and alerting them to risks while traveling? ☐ ☐
- Is there a plan to support the executives and families in the event of medical or security need, irrespective of location? ☐ ☐

Insider Threat

- Have we conducted an insider threat audit? ☐ ☐
- Is there a recurring process to review/evaluate who has access to important information in the organisation? ☐ ☐

Emergency Response

- Is there a documented emergency response plan for various scenarios at home and abroad (e.g., medical emergencies, security threats)? ☐ ☐
- Are executives and family members regularly trained on emergency procedures? ☐ ☐

Cyber Security

Network

Yes

No

- Are the executives' home networks protected by enterprise-grade firewalls and intrusion detection systems?
- Is there a regular schedule for network vulnerability assessments and penetration testing?

☐
☐
☐
☐

Data Protection

- Is all sensitive data encrypted, both in transit and at rest?
- Are there strict access controls in place for confidential information?

☐
☐
☐
☐

Device Management

- Is there a mobile device management (MDM) solution in place for all executive devices and those of their family members?
- Are all devices (phones, laptops, tablets, etc.) equipped with up-to-date antivirus and anti-malware software?

☐
☐
☐
☐

Travel

- Are executives utilising proper security protocols for their devices when traveling?
- Are we conducting TSCM bug sweeps where the executives are staying during travel?

☐
☐
☐
☐

Incident Response

- Is there a documented incident response plan for ransomware and other cyber attacks?
- Has the plan been tested through simulations or tabletop exercises?
- Are our network and devices monitored 24×7, backstopped by on-call cyber engineers to defeat malware and restore network and device functionality?

☐
☐
☐
☐
☐
☐

General Security Practices

Security Awareness Training

Yes No

- Is there a regular schedule of security awareness training for executives and their family members?
- Does the training cover both physical and cyber security topics?

☐ ☐
☐ ☐

Risk Assessment

- Is there an annual formal risk assessment process that covers all aspects of executive security?
- Are we investigating all threats to verify their legitimacy to take action appropriately?
- Are the results of these assessments used to update security protocols?

☐ ☐
☐ ☐
☐ ☐

Insurance Coverage

- Is there comprehensive insurance coverage for cyber incidents, kidnap and ransom, and other security-related risks?
- Is the coverage regularly reviewed and updated?

☐ ☐
☐ ☐

Governance


- Is there a designated security officer or team responsible for overseeing all aspects of executive security?
- Do we have a trusted partner on both the digital and physical sides to help us triage and respond to executive threats?
- Do our vendors have response capabilities with real rigor and have they been tested through simulation/tabletop exercises?
- Are there regular security briefings for executives and their family members?

☐ ☐
☐ ☐
☐ ☐
☐ ☐


Discuss your security requirements

To discuss your organisation's requirements or request a tailored assessment, contact our team at:

info@solaceglobal.com or solaceglobal.com



Solace Global Risk, part of Global Guardian, provides integrated security solutions that protect senior leaders, personnel, and operations worldwide. Our approach brings together intelligence, travel risk technology, journey management, executive protection, and 24/7 oversight into one continuously connected system.

We support corporate, government, NGO, and family office clients across routine travel, complex environments, and high-profile engagements, enabling organisations to move people safely while maintaining visibility and control.

Why organisations choose Solace Global

One unified solution for global mobility

Executive protection, journey management, intelligence, and travel security technology delivered as one coordinated capability rather than separate services.

24/7 operational oversight

Continuous monitoring and support from dedicated Global Security Operations Centres, ensuring assistance is always available when plans change.

Intelligence-led decision support

Timely, relevant insight that informs planning, routing, and protective measures before and during travel or public activity.

Advanced travel security technology

Live location visibility, near real-time alerts, pre-travel intelligence, and SOS connectivity to our GSOC to support travellers before, during, and after their journeys.

[Learn more](#)