Executive Risk Consideration Checklist

With so much personal data available on social media and other online platforms, the risks to executives have broadened, exposing them to reputational damage, cyber-attacks, fraud, and physical harm. Personal details shared online can be weaponized, making it critical to identify legitimate threats quickly. This checklist helps you explore and discuss the risk level of high-profile individuals within your organization and understand if a detailed vulnerability assessment is warranted.

Company and Executive Risks

Understanding the potential risks faced by your company and its executives requires a close examination of their digital presence, physical vulnerabilities, and access to sensitive information. Consider the following factors to assess your exposure:

Social Media / Digital Presence

- [ ] Do the executive or their family members have public social media accounts, or participate in online communities, forums or chatrooms?
- [ ] Have they been featured in recent news articles or made public appearances that increase their visibility or have they expressed opinions on controversial topics that may cause outrage or motivated attacks?
- [ ] Does the executive have access to sensitive information or decision-making power?

Physical Vulnerabilities

- [ ] Does the individual participate in corporate, media, or speaking events for which schedules are available online?
- [ ] Is information, including addresses and interior or exterior photos, of the executive's home or office locations available online?
- [ ] Does the executive frequently travel, particularly to regions with higher security risks?

Digital Vulnerabilities

- [ ] Does the company deal with critical infrastructure, sensitive IP, sensitive data, or operates in a high-risk industry (e.g., finance, healthcare, technology) that would be attractive to a threat actor?
- [ ] Is the executive's or their family's personal information easily found online (e.g., on social media or in data breaches)?
- [ ] Are there past incidents of personal data exposure involving the executive or their family?

Executive Risk Consideration Checklist

Risk Assessment Outcome

A thorough risk assessment highlights the various ways executives and their families are exposed to both digital and physical threats. Key findings would include:

Pattern of Life Exposure

Information shared by employees or their family members through social media and other digital platforms can inadvertently reveal patterns of daily activities. Threat actors exploit this data to enable stalking, surveillance, and harassment.

Personally Identifiable Information (PII)

The unintended exposure of personal information continues to pose significant risks to executives. Threat actors can leverage a wide array of data—such as utility records, voting records, property ownership, and campaign donations—to target individuals.

Doxxing

The deliberate publication of sensitive or personally identifiable information online has become a common tactic for blackmailing, threatening, and intimidating executives and their families.

Credential Theft

C-suite credentials are among the most valuable targets for cybercriminals, as they provide access to highly sensitive information. Poor password hygiene, credential reuse, and engagement with unsecure websites further increase vulnerability

Next Steps

Taking the right steps to protect executives and key personnel begins with a clear plan, actionable insights, and ongoing risk management. Here's how to move forward:

- **Consultation and Planning:** Begin by scheduling an initial consultation to discuss the assessment process, address any questions, and outline your objectives. Once aligned, finalize the timeline and steps for completing the full assessment.
- **Report and Recommendations:** Upon completion of the assessment, receive a detailed report outlining findings and tailored security recommendations. These insights will help you monitor identified risks and prioritize actions to address vulnerabilities.
- **Risk Reduction:** Take proactive steps to reduce risk, including the removal of personally identifiable information (PII) from online databases. Implement the recommended actions to enhance the executive's digital security, and continue monitoring risks to stay ahead of potential threats.

About Nisos®

Nisos, the Managed Intelligence Company®, is a trusted digital investigations partner specializing in unmasking human risk. We operate as an extension of security, risk, legal, people strategy, and trust and safety teams to protect their people and their business. Our open source intelligence services help enterprise teams mitigate risk, make critical decisions, and impose real world consequences.