ONTIC

CHECKLIST

How to Assess Your Executive's Digital Footprint to Identify Threats

It's alarmingly easy for threat actors to access an executive's personal details through simple online data scraping or a quick dive into their presence in the ever-expanding social media ecosystem. Beyond that, any personal information shared by their family members, friends, children's caregivers, or anyone related to their inner circles can tip off someone aiming to harm an executive or their reputation.

This checklist will help enhance your understanding of your executive's digital footprint by covering what's visible online, frequently overlooked vulnerabilities, and immediate steps you can take to mitigate risks.

What Information Is Visible Online?

It's vital you establish a baseline so you know how to find potential weak spots and where to focus your attention.

☐	**Are your executive's personal information and work tied to their social media accounts? If so, does your organization's marketing or PR team post content on social media under the executive's name?** e.g., LinkedIn, Instagram, X (formerly Twitter)
☐	**Does your executive actively publish content and engage with their social media accounts? If so, do they share personal photos and information that could inadvertently put them at risk?** e.g., a home photo with their address number visible
☐	**Does your executive have any "secret" or alias social media accounts? If so, what are their handles or profiles?**
☐	**Does the executive's partner and/or children regularly post content on social media? If so, do they share or engage with controversial or political content?**
☐	**Does the executive, their family, or their friends use location-based check-ins or share geo-tagged content on social media? If so, how often?**
☐	**Has your executive posted reviews on product or company sites?** e.g., Amazon, Glassdoor
☐	**How does your executive travel?** e.g., personal aircraft, yacht, fractional jet service, helicopter, Uber, public transportation
☐	**Are their travel service providers and vendors maintaining confidentiality and taking the necessary precautions to keep them safe?** Keep in mind that even exposing an aircraft's tail number in a photo could create a vulnerability
☐	**Is the executive or their family's charitable and political donations publicly available?**

Continued	
☐	**Does your executive belong to any boards or publicly support charities, political parties, or causes? If so, which ones?**
☐	**Is the executive publicly known to have any controversial opinions or taken any controversial actions? Have they or anyone in their network shared this information online?**
☐	**What news and press mentions are available online about the executive? Are any negative news mentions tied to the executive or their immediate family?**

PRO TIP:
Executives sometimes have a false sense of security or anonymity and don't always realize that certain information is publicly available or someone wishes them harm. By gathering a baseline understanding of what is visible and the sentiments others share about them online, you can provide the custom monitoring, recommendations, and protective measures they need. Ensure you're using the most recent, accurate, and vetted data to take the right action.

Where Are the Cracks?

Be sure to consider commonly overlooked vulnerabilities so you can take the proper steps to improve the executive's safety and the safety of their inner circle.

☐	**How predictable is your executive's day-to-day and/or travel schedule? Does anyone in their inner circle share information online that may expose elements of their routines?** e.g., a local business they regularly patronize or a hotel where they frequently stay
☐	**Does the executive have an assistant who is active on social media? Does the assistant's LinkedIn or other social media profiles publicly display that they work for the CEO or company? Are they inadvertently sharing confidential travel information on their personal social media accounts?**
☐	**Where does your executive regularly purchase products or services? Are vendors aware they must ask permission to share content around the executive's patronage?**
☐	**Do family members or other members of their inner circle post locations of an executive's private residence, vacation destinations, or children's schools?** Keep in mind that even an image of a front yard or a photo with identifiable buildings or vehicle license plates can be used to track the location of an executive or a member of their inner circle
☐	**Has your executive been "doxxed" (i.e., has someone publicly exposed identifying information about the executive without their consent as a form of online harassment?) If so, when and why?**
☐	**Do your data sources combine coverage of identity, criminal activity, civil litigation, adverse media, and global intelligence records to gain a thorough understanding of a POI?**

PRO TIP:
New social media sites, data brokers, and people search services emerge all the time. Manually combing and removing information from these sites can require significant time and energy. Leveraging investigative research software can help streamline by giving you the power to customize your monitoring for each executive and pull relevant mentions, posts, tweets, and other signals. Workflows can be configured to support most needs and use cases, creating a triage approach. This way, you'll be alerted when something requires your attention and can take immediate action.

What Can You Improve?

Uplevel your security by digging deeper and taking advanced steps to protect executives online and in person.

☐	**Who is in your executive's ecosystem, and do they pose any risks?** Tracking your principal/executive is not enough; family and friends often create vulnerabilities without realizing they've done something wrong
☐	**What quick and easy steps can you take to remove sensitive information online?** e.g., blurring the executive's residence on Google Street View using reputable services like Reputation Defender
☐	**Is there a framework built to determine who can enter your executive's circle and what actions they must take or avoid to keep the executive and their family safe?**
☐	**Are there any assets currently in the executive's name that should be in the company's name instead?** e.g., purchasing a new property
☐	**Does the executive have policies and procedures to restrict or prohibit guests from posting pictures on social media when they host events at their residence?** e.g., some public figures have a "no phones allowed" policy at events they host and may even ask guests to surrender devices upon entry to mitigate risks
☐	**Are there policies and procedures in place to prohibit vendors such as landscapers or housekeepers from posting pictures on social media?**
☐	**Do your data sources deliver both real-time and historical data for a holistic view of POI background and activities?** This is critical for creating an in-depth entity profile on any threat to your executive
☐	**Is your research on potential threat actors automated, and are you continuously monitoring for POI activity updates?** Automated research increases your team's ability to uncover critical signals, gain a comprehensive view of threats to your principal, and take early action
☐	**Do you have any actionable workflows you can execute when a POI or threat surfaces?**

PRO TIP:
Sometimes, the information you discover can be uncomfortable to discuss. Remember to be sensitive when presenting findings to executives, especially when it involves family members, and maintain an unbiased approach.

Even with the best tools, monitoring an executive's digital footprint will never be a "set it and forget it" effort. By adopting Ontic's Integrated Research solution to run these processes, you can ensure you're covering all the necessary bases, create standardized incident triage workflows, and benefit from automated data analyses and insights. **Learn More >**

ONTIC