Constella

Executive Digital Risk Protection Checklist

A Comprehensive Guide to Protecting Executive Digital Footprints

Executives are high-value targets for cybercriminals, bad actors, and even corporate adversaries. The more information available online, the greater the risk of cyberattacks, reputational damage, and even physical threats.

Use this checklist to evaluate current vulnerabilities and implement proactive security measures to safeguard executives' personal and professional digital presence.

---

1. Digital Footprint Assessment

- ☑ Conduct a search for the executive's name using various search engines to identify publicly available information.
- ☑ Review the executive's online presence (company website, media mentions, social media profiles).
- ☑ Check data broker sites (such as Whitepages, Spokeo, and PeopleFinder) for exposed personal information.
- ☑ Audit previous data breaches using services like dark web monitoring tools.
- ☑ Remove or minimize personal information from company press releases, public filings, and social media.

2. Cybersecurity & Digital Identity Protection

- ☑ Use unique, complex passwords for all personal and corporate accounts (consider a password manager).
- ☑ Enable Multi-Factor Authentication (MFA) on all email, banking, and corporate accounts.
- ☑ Regularly update security settings on personal and professional social media accounts.
- ☑ Use a separate, secure email account for sensitive communications.
- ☑ Disable location tracking on social media and mobile apps.

3. Social Media & Online Presence Security

- ☑ Set social media profiles (Facebook, LinkedIn, Twitter, Instagram) to private or restricted.
- ☑ Remove personal information, including birthdays, family members, and home locations, from public profiles.
- ☑ Avoid posting activities or plans and real-time location updates.
- ☑ Monitor impersonation attempts on LinkedIn and other platforms.
- ☑ Use a separate, business-only LinkedIn profile to minimize exposure.

4. Digital Threat Monitoring & Proactive Defense

- ☑ Implement real-time dark web monitoring to detect compromised credentials and identity leaks.
- ☑ Set up Google Alerts for mentions of the executive's name across the web.
- ☑ Conduct regular scans for executive impersonation attempts or fraudulent accounts.
- ** ☑ Use AI-driven threat intelligence solutions to detect emerging risks.
- ☑ Work with cybersecurity professionals to conduct quarterly security audits.

5. Physical Security & Executive Travel Safety

- ☑ Remove home address and personal contact details from public directories.
- ** ☑ Ensure executives use alias names for hotel and travel bookings to avoid tracking.
- ☑ Avoid using personal devices on public Wi-Fi networks without a VPN.
- ☑ Establish secure transportation and travel security protocols for high-risk destinations.
- ☑ Educate executive assistants and family members on security best practices.

6. Insider Threat Prevention & Company-Wide Awareness

- ☑ Limit access to executive data—only authorized personnel should have sensitive details.
- ☑ Implement a need-to-know policy for executive schedules and corporate communications.
- ☑ Conduct cybersecurity training for executives and their teams on phishing, social engineering, and digital threats.
- ☑ Monitor for internal security threats (disgruntled employees, data leaks, and unauthorized access attempts).
- ** ☑ Establish an executive security incident response plan for rapid action in case of a breach.

Next Steps: Take Action to Secure Your Executive Team

The best defense is a proactive strategy. Regularly reviewing and updating executive security practices can prevent cyber threats, reputation damage, and real-world risks.

Constella Hunter+ delivers comprehensive, automated digital risk protection, including:

- ✓ 24/7 monitoring of surface, deep, and dark web threats
- ✓ Real-time alerts for exposed credentials, impersonation, and cyber risks
- ✓ Seamless integration with SOC and security response workflows