



Executive OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

This checklist is designed for executives, board members, public-facing leaders, and other high-value individuals (VIPs). It focuses on publicly observable open-source intelligence (OSINT) signals that increase the risk of doxxing, impersonation, targeted phishing, fraud, and physical approach. It reflects what a motivated external actor can learn without privileged access.

How to use: Review each item, mark Priority (H/M/L) based on potential impact, and mark Status (OK/Fix/N/A) based on current state. Keep evidence (URLs, screenshots, notes) in your internal case file.

Executive / Leader Name: **Date:**

Role / Title: **Organization:**

Assessor / Point of Contact: **Review Type:**

Notes (optional):

1) Identity, Address, and Contact Exposure

Focus: discoverable name variants, addresses, phone numbers, emails, and linkable identifiers.

Home address is not easily tied to the executive's name through common people-search sites.

Priority: H M L

Status: OK Fix N/A

Prior addresses are minimized (opt-outs completed where possible).

Priority: H M L

Status: OK Fix N/A

Personal phone number is not publicly listed on bios, profiles, directories, or press pages.

Priority: H M L

Status: OK Fix N/A

Reverse phone/email lookups do not reliably map to the executive or a home address.

Priority: H M L

Status: OK Fix N/A

Public contact routes use controlled aliases (not personal email/phone) and are monitored.

Priority: H M L

Status: OK Fix N/A

Full date of birth, middle name, and other correlation details are not publicly exposed.

Priority: H M L

Status: OK Fix N/A

Family relationships are not easily inferred via public profiles, tagged posts, or "family tree" sites.

Priority: H M L

Status: OK Fix N/A



Executive OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

2) Data Broker and People-Search Suppression

Focus: high-leverage opt-outs that reduce doxxing speed and targeting accuracy.

- Top people-search/data broker listings reviewed for the executive and key family members.

Priority: H M L

Status: OK Fix N/A

- Suppression/opt-out requests submitted and documented (site, date, confirmation).

Priority: H M L

Status: OK Fix N/A

- Search results re-checked after opt-outs for residual cache/index exposure.

Priority: H M L

Status: OK Fix N/A

- Name variants checked (middle initial, alternate spellings, prior names).

Priority: H M L

Status: OK Fix N/A

- Old resumes, speaker bios, PDFs, and third-party profiles containing personal details removed or de-indexed where feasible.

Priority: H M L

Status: OK Fix N/A

3) Social Media and Public Profile Hygiene

Focus: what an attacker can infer from posts: location, routine, relationships, access, and assets.

- All major platforms reviewed (LinkedIn, X, Facebook, Instagram, TikTok, YouTube, etc.).

Priority: H M L

Status: OK Fix N/A

- Privacy settings verified (followers/friends lists, tagged photos, contact details restricted).

Priority: H M L

Status: OK Fix N/A

- Geotagging disabled; location history and check-in features minimized.

Priority: H M L

Status: OK Fix N/A

- No real-time travel/location posting until after returning.

Priority: H M L

Status: OK Fix N/A

- Older posts reviewed for home identifiers (street signs, house numbers, landmarks, school logos).

Priority: H M L

Status: OK Fix N/A

- Family member accounts reviewed for cross-linking, tagging habits, and accidental exposure.

Priority: H M L

Status: OK Fix N/A

- Profile images/banners do not reveal sensitive context (badges, office layout, access points, whiteboards).

Priority: H M L

Status: OK Fix N/A



Executive OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

4) Professional, Corporate, and Public Records

Focus: filings, directories, and disclosures that can leak residential address or personal contact details.

Corporate filings/registries do not list residential address or personal phone/email.

Priority: H M L

Status: OK Fix N/A

Registered agent and business addresses use controlled addresses (not residential).

Priority: H M L

Status: OK Fix N/A

Professional directories and licensing sites checked for address/phone exposure.

Priority: H M L

Status: OK Fix N/A

Board memberships and public rosters reviewed for sensitive disclosures.

Priority: H M L

Status: OK Fix N/A

Press releases and "About" pages avoid personal contact details and predictable routine information.

Priority: H M L

Status: OK Fix N/A

Property-related public records reviewed for direct linkage to home address where feasible (risk-based).

Priority: H M L

Status: OK Fix N/A

5) Credential, Breach, and Account Exposure

Focus: signals that enable impersonation, account takeover, and targeted phishing.

Known breach exposures checked for executive emails/usernames; remediation tracked.

Priority: H M L

Status: OK Fix N/A

Password manager in use; no password reuse across personal and business services.

Priority: H M L

Status: OK Fix N/A

MFA enabled on critical accounts (email, social, cloud, finance) using an authenticator app or hardware keys.

Priority: H M L

Status: OK Fix N/A

SMS-based MFA minimized; recovery numbers hardened against SIM-swap where possible.

Priority: H M L

Status: OK Fix N/A

Account recovery questions are not guessable from OSINT (schools, pets, hometown, etc.).

Priority: H M L

Status: OK Fix N/A

Public usernames are not reused across platforms (reduces correlation and impersonation).

Priority: H M L

Status: OK Fix N/A



Executive OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

6) Documents, Photos, and Metadata Leakage

Focus: PDF metadata and image EXIF that can quietly reveal identity, location, or internal systems.

Public PDFs reviewed for metadata (author name, username, internal paths, timestamps).

Priority: H M L

Status: OK Fix N/A

Images reviewed for EXIF data (GPS, device model); EXIF stripping enabled for publishing.

Priority: H M L

Status: OK Fix N/A

Public file shares reviewed for access scope; stale/overly permissive links removed.

Priority: H M L

Status: OK Fix N/A

Slide decks and conference materials reviewed for embedded links, hidden notes, and comments.

Priority: H M L

Status: OK Fix N/A

Backgrounds in video calls/photos checked for sensitive details (documents, badges, layouts, addresses).

Priority: H M L

Status: OK Fix N/A

7) Family, Assistants, and Associate Exposure

Focus: indirect exposure through close contacts that adversaries exploit.

Executive assistant/admin contact paths are controlled (no public posting of personal numbers).

Priority: H M L

Status: OK Fix N/A

Family member profiles checked for address/phone, school information, and routine posts.

Priority: H M L

Status: OK Fix N/A

Tagging practices controlled (avoid linking family + location + timing).

Priority: H M L

Status: OK Fix N/A

Emergency contacts, personal schedules, and calendar artifacts are not publicly posted or searchable.

Priority: H M L

Status: OK Fix N/A

Known "trusted circle" members understand impersonation and verification expectations.

Priority: H M L

Status: OK Fix N/A

