



Executive Digital Exposure Trends: Understand and Reduce Your Risk

nisos.com

tel: 703-382-8400

2101 Wilson Blvd. Suite 304

Arlington, VA 22201

Table of Contents

Introduction	3
Key Findings	4
Executive Summary	5
Physical Vulnerabilities	6
• Geolocation Data & Proximity Risk	7
• Geolocation Data & Fitness Applications	8
Social Media Exposures	10
• Imposters & Account Takeovers	11
• Proximity Risk	12
Digital Vulnerabilities	14
PII Exposures and Removals	17
Conclusion	19

Introduction

In January, Nisos [reported](#) that in the six weeks after the fatal shooting of the UnitedHealthcare CEO, our analysts detected 2,200 threats towards executives - 41% more than the total of the previous six months. We embarked on our latest research project to raise awareness of common vulnerabilities among executives and educate about how to reduce risks.

Nisos has provided clients with protective intelligence and executive protection for years. In this inaugural executive vulnerabilities report, we examine the evolving threat landscape and assess risk trends across our client base. Our goal is to shed light on how the digital world exposes high-profile individuals and to identify actionable steps for strengthening executive security.

Key Findings

98%

of company executives had property addresses publicly linked to their name in public records or people search sites

58%

of executives had their Social Security number (SSN) compromised in breach data

100%

of executives had breach data exposed linking their name to at least 1 current email address

20%

of executives' public social media accounts revealed personal details including personal relationships, important dates such as birthdays, and, in some cases, travel details.

Executives' immediate family members had **an average of 6** social media accounts that revealed personal and family information



Executive Summary

The following trend analysis represents a sample of 50 Executive Vulnerability Assessments (EVA) Nisos conducted through 2024 and early 2025 for executives across a random distribution of industries and locations.

This report focuses on four key areas

Physical Location Data

Digital Footprint

Social Media Activity

PII Exposure

We identified digital exposures that can lead to possible physical risks and cyber vulnerabilities for executives and their families. We identified social media, breach data, and sites hosting personally identifiable information (PII) as key sources revealing personal information a threat actor can use to target an executive's family, property, or accounts. Through this report, we aim to equip organizations with the insights needed to protect their leaders in an increasingly connected world.



Physical Vulnerabilities

Threat actors intent on physically confronting a target or entering their home—with or without the executive present—can often identify addresses and property layouts in public information. Depending upon the state or county in which an executive lives, permits, tax documents, parcel registration, and popular realtor or home ownership sites also often include accessible address information, as do business registration documents an executive or family member may have filed using their real address.

98%

of company executives had property addresses publicly linked to their name in public records or people search sites

92%

had publicly viewable exterior images

88%

had interior photos or floor plans available on popular realtor sites

- *This information can help threat actors gain an understanding of a property's layout before a physical confrontation.*

82%

had their address available in public business registration, voter roll data, or political/philanthropic donations

- *Registration and donation information are often considered public record and are not easily removable.*



Physical Vulnerabilities

Geolocation Data & Proximity Risk

Social media and applications such as fitness trackers can provide real-time location information for an executive and their family.

Geotagging and live posts on social media can provide threat actors with enough information to target an executive, intercept their next destination, and identify when their home is unoccupied or children are unattended.

While only **16%** of executives shared geotagged information themselves, **20%** of their family members shared information related to the executives' location.



Approximately **30%** of surveyed executives and their family members shared geolocation and pattern-of-life information through public reviews.

Physical Vulnerabilities

Geolocation Data & Fitness Applications

Public fitness tracking applications can display frequented exercise routes, home addresses, and predictable workout routines.

1 of our client executives publicly shared geolocation information through popular exercise applications, while family members of **5** executives did so.

The geolocation information often included routes that started or stopped at the executive's home address. This data also conveyed frequented routes and predictable exercise times giving threat actors insight into when they can possibly confront an executive or their family member.

From our sample, doxxing only occurred in **4%** of cases - with each instance carried out with malicious intent.

Such an event is generally a low probability for most executives. However, when it happens, it indicates malicious intent and targeting and can have a significant impact on an executive's life and even safety.



Physical Vulnerabilities

What Can You Do?



Claim ownership of addresses on popular realtor sites, and request ownership attribution and property image removals.



Avoid putting a home address on political/philanthropic donations and business registrations, and use a registered agent when registering businesses when possible.



Avoid using personal or attributable names for home WiFi networks, external decorations, or other publicly viewable infrastructure.

Social Media Exposures

Public social media profiles provide nefarious actors access to a target's personal life. Available information can support impersonation, financial fraud, or physical confrontations. For example, names of pets or family members, important dates, and associated schools or institutions can provide threat actors with answers to common security questions on sensitive accounts. With enough available information, a threat actor can identify a target's circle of trust and understand the executive's network. In some cases, the amount of family information available through social media profiles negates a threat actor's need to use alternative platforms, such as people search websites or breach information.

We identified an average of just over
3 public mainstream social media accounts per
executive, on which approximately
20% revealed personal information.

3 public social media accounts were
identified per executive



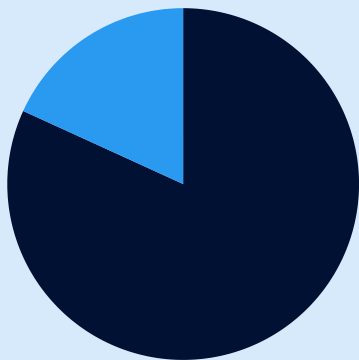
Public information included family pictures; searchable friends lists; home exteriors and interiors; important dates, such as family birthdays, anniversaries, or graduations; children's schools, hobbies, and extracurricular activities; announcements of conferences they would attend; indications the executive was on vacation, suggesting their home was unoccupied; exercise routes; geotagged posts of their live location; interactions with antagonistic actors; and political or other posts that some viewers possibly deem controversial.

Social Media Exposures

Imposters & Account Takeovers

Imposter profiles and dated accounts can harm an executive's image and reputation through threat actor takeovers and reused content. Many people own multiple social media accounts they have not used for an extended period of time and have likely forgotten about.

These old, unused accounts often contain dated and weak passwords, and therefore may be accessible through exposed breach data. This presents threat actors an opportunity to take over the account and post posing as the executive, which can cause reputational and other harm.



18%

of executives surveyed were the target of imposter accounts on social media, most of which were used to support financial scams and conduct social engineering on unsuspecting victims.

Deleting unused accounts inhibits the threat of account takeovers and reduces the amount of available content fraud actors can use in their schemes.

Social Media Exposures

Proximity Risk

Public social media accounts for executives' immediate family members—including spouses, former spouses, and children—frequently represent the most complete access to an executive's personal life.

Immediate family members are often easily identifiable through official company posts, documents, or engagement, meaning their online activity expands the executive's attack surface.

Immediate family members maintained an average of
6 public mainstream social media accounts.

Their accounts exposed similar images and geolocation information as executive accounts but often at a higher frequency.



Threat actors can often acquire unique information from public social media comments posted by a target's close friends or family. Extended, often elderly, family members can overshare information, such as mentioning a minor child's name in a comment on an executive's public photo. This information enables threat actors to identify physical locations—such as schools or sports venues—through posts about children's activities and event schedules. This increases the risk of a physical confrontation with an executive or their family.

Social Media Exposures

What Can You Do?



Increase the privacy settings on all family social media accounts to inhibit threat actor insight, contact, and harassment.



Avoid geotagging locations or indicating times when away from home, as threat actors can use this information to support physical confrontations or property raids.



Review comments and other engagement on social media to monitor for family members or friends who overshare your information, such as identifying children in photo comments or posting pictures of an event at your home.



Operate social media use as if all posts are public, including limiting images of homes, family members, pets, or other pattern-of-life information that can provide insight into physical locations or common security questions.



Delete all unused accounts to inhibit possible account takeovers.

Digital Vulnerabilities

Data breaches are becoming more common, and it's easier than ever for threat actors to obtain sensitive biographical, financial, or contact information.

Recent breaches involving major companies and organizations have likely increased the overall threat landscape to an executive and their family.

While portions of an individual's personal data were once fragmented across multiple breaches, recent large-scale breaches and the continued threat of other major exposures enables threat actors to easily acquire data that previously would have required significant effort, potential cost, and research time.



Digital Vulnerabilities

Executive Vulnerabilities

58%

of executives had their SSN compromised in breach data

90%

of executives had at least one plaintext password exposed in breach data

Each executive averaged approximately 3 exposed plaintext passwords.

72%

had their SSN listed for sale on a popular dark web marketplace

100%

of executives had breach data linking their name to at least one past or current email address

Each executive had an average of approximately 4 email addresses exposed in breach data and approximately 3 telephone numbers.

Proximity Risk: Executives' Family Members

26%

of our executive clients' spouses* had their SSN exposed in breach data

39%

of executive clients' spouses* had their SSN listed for sale on a popular dark web marketplace

70%

of executives had immediate family members' personal or contact information exposed in breach data

This creates additional possible targets for nefarious actors, additional contact methods, or means to confirm an executive's suspected address.

**Of the 86% of executives who had a spouse at the time of the risk assessment*

Digital Vulnerabilities

What Can You Do?



Remain alert for suspicious activity that can indicate fraudulent use of exposed SSNs.



Consider freezing credit to protect against fraudulent activity in the case that sensitive information becomes compromised.



Ensure known compromised passwords, simple passwords, or ones used across multiple accounts are no longer in use.



Use unique passwords for all accounts.



Maintain awareness of any exposed email addresses and phone numbers enabling possible phishing attempts.

PII Exposures and Removals

People search sites, public data brokers, and business search sites are among the sources that host a person's PII. Not all, but many of these sources are available to the public for free and can provide threat actors with personal information including dates of birth, residential addresses, the names and dates of birth of family members, a person's email addresses and phone numbers, as well as business-related information and employment history. It is possible to reduce the number of sites hosting an executive's PII by submitting removal requests, often repeatedly and over time.

We found an average of 95 instances of PII over approximately 200 popular PII sites.

PII Exposures and Removals

What Can You Do?



Request PII removals for all current residential or contact information available on popular people search sites, databases, and data aggregators.



Regularly check and resubmit removal requests, particularly as data can repopulate on sites or may not be removed after a single request.

Real World PII Risk Reduction is (hard but) Possible

The challenge with PII is its broad availability and difficulty in permanently removing it from the public realm.

We were able to submit removal requests on behalf of clients to an average of 73 sites. Remaining websites required the executive to provide proof-of-identity documentation, and we provided removal guidance and support to the executive's team to submit these removal requests.

Of the sites for which we submitted removal requests, 70% were successful in our first round of removals. This represented a 54% overall reduction of the executive's PII. The client removal requests reduce their publicly exposed PII—and thereby risk—even further. We recommend ongoing PII identification and removal request submissions.

Conclusion

Executives are uniquely vulnerable in today's evolving threat environment. As public-facing figures with access to sensitive information, strategic insight, and decision-making authority, they represent high-value targets for adversaries seeking to exploit organizations through both personal and professional channels.

Modern protection must go beyond physical security to include digital risk management. Understanding how attacks unfold, and the publicly available information that fuels them, is critical to reducing exposure and enhancing an executive's security posture.

Our analysis of executive clients highlights common digital exposure trends a threat actor may use to target an executive and their family, property, or accounts. Personal identifiers, location data, family information, and professional affiliations can pose possible physical, digital, and reputational risks for executives and their families. These risk trends can provide threat actors with sufficient information in their targeting considerations, possibly also enabling fraud and account theft.

To strengthen an executive's security posture, organizations must take deliberate steps to reduce exposure. To mitigate these risks, we recommend ensuring social media accounts are set to private, regularly removing PII from hosting websites, and maintaining ongoing awareness of where an executive's personal information exists online.

About Nisos®

Nisos is the human risk management company specializing in unmasking threats before they escalate. We are a trusted advisor who operates as an extension of security, intelligence, legal, and human resource teams to protect their people and business. Our intelligence-led solutions help enterprises make critical decisions, manage human risk, and drive real world consequences for digital threats.

For more information visit: www.nisos.com
email: info@nisos.com

call: +1-703-382-8400
follow: [LinkedIn](#)

