Research

Leadership at Risk in a Data-Exposed World

Why Your C-suite's Digital Footprint Is Your Biggest Blind Spot

2025 snapshot of the exposure of more than 10,000 C-suite executives in the USA across different sectors and how compromised privacy impacts cyber and physical security.

VanishID.

vanishid.com

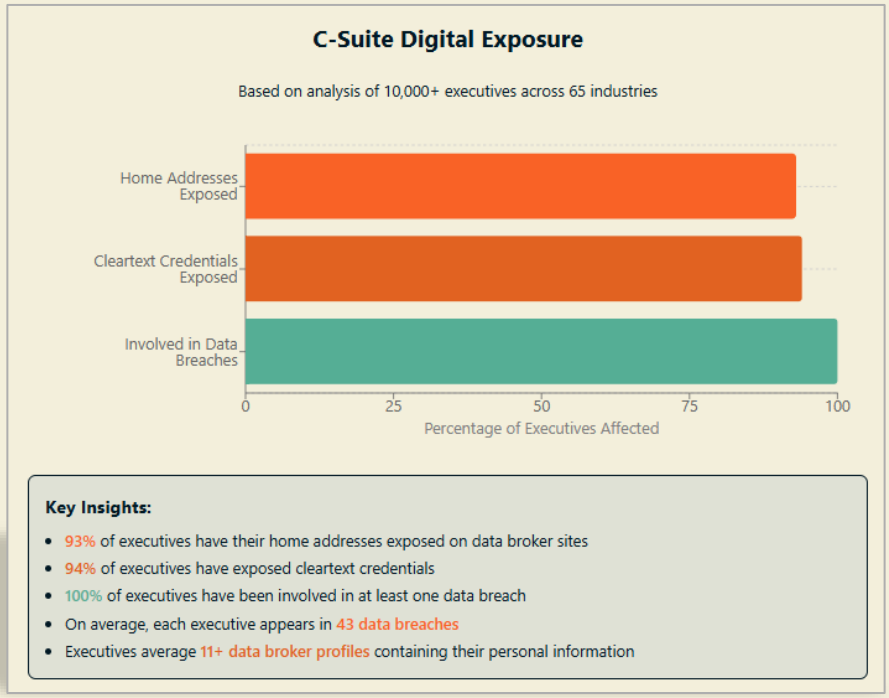
Executive Summary

The numbers tell a troubling story: **93% of C-suite executives have their home addresses exposed on data broker sites. 94% have plaintext passwords available to attackers. 100% have been caught in data breaches** — with an average of 43 breaches per executive.

These statistics represent real, exploitable pathways to both cyber and physical threats.

VanishID's analysis of over 10,000 U.S.-based executives across 65 industries reveals the true extent of this crisis. Our research encompasses leaders from 411 Fortune 500 and 1,329 Global 2,000 companies, providing unprecedented visibility into executive digital vulnerability.

This paper examines how exposed personally identifiable information (PII) creates tangible risks for executives and their organizations, which leadership roles face the greatest danger, and how security teams can implement effective digital executive protection programs to address these threats.



Index

What the Data Reveals

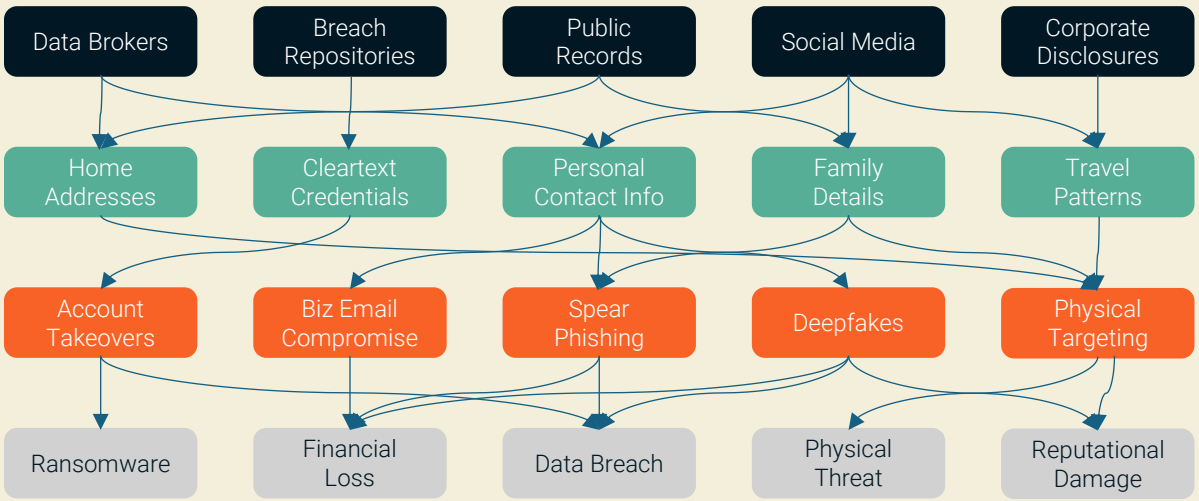
Our research into executive digital footprints uncovered alarming exposure patterns:

Type of Exposure	Percentage of Executives Affected	Key Data Point
Home Address Exposure	93%	11 data broker profiles per executive
Data Breach Involvement	100%	43 data breaches per executive
Cleartext Credentials	94%	4.3 exposed credentials per executive
Personal vs. Corporate Breaches	84%	Exposed passwords come from personal breaches

Executives' information spreads across multiple channels:

- **Data broker sites** that aggregate and sell personal information
- **Breach repositories** containing stolen credentials and personal data
- **Public records** including property ownership, court filings, and licenses
- **Social media platforms** revealing personal details, connections, and activities
- **Corporate disclosures** in SEC filings, press releases, and company websites

What makes this exposure particularly dangerous is how these information sources combine to create comprehensive profiles of executives — providing attackers with all they need to target both digital accounts and physical locations.



Real-World Example: The Security Expert Who Wasn't Secure

Consider what happened when *Robert M. Lee*, a recognized cybersecurity authority (Security Executive of the Year for 2022 by SC Media) and CEO of Dragos, volunteered for a live hacking demonstration sponsored by VanishID. Despite his expertise, ethical hacker and CEO of SocialProof Security, *Rachel Tobac*, successfully targeted him using only publicly available information.

Tobac's approach illustrates exactly how attackers exploit executive digital footprints:

1. She gathered Lee's contact details (phone numbers, addresses, email addresses) from public data broker sites
2. As a result, she identified his involvement in 12 data breaches, which exposed his personal information
3. She also found a short video clip from social media that allowed her to create a voice clone

With this foundation, Tobac went to work on multiple attack vectors:

- **Caller ID spoofing** to make calls appear to come from Lee
- **Voice cloning** to call a team member and request Lee's password manager master password
- **Targeted phishing emails** using personal information to create convincing messages
- **Deepfake creation** that could impersonate Lee in video conferences

This wasn't a hypothetical exercise: Tobac demonstrated real capabilities available to motivated attackers. You can watch the ~4-minute exposé here.

How Digital Exposure Creates Real-World Risks

Physical Security Implications

Compromised personal data privacy leads to compromised physical security because digital exposure directly translates to physical vulnerability. To make matters worse, freemium apps like https://famylocate.app and similar commercial OSINT tools can geo-locate a person instantly by knowing their mobile phone number. Digital exposure enables physical security threats such as:

- **Home targeting:** With 93% of executives having exposed addresses, their residences become potential targets for harassment, surveillance, or intrusion.
- **Family vulnerability:** Information about spouses, children, and other family members allows attackers to target executives' loved ones as leverage points.
- **Travel pattern exposure:** Public schedules, social media activity, and location data can reveal when executives are away from home or traveling abroad.
- **Stalking and harassment:** Exposed contact information facilitates unwanted contact and potential harassment campaigns.

Real-World Cases: When Digital Exposure Becomes Physical Danger

Case 1: Assassination of UnitedHealthcare CEO

On December 4, 2024, Brian Thompson, CEO of UnitedHealthcare, was fatally shot outside the New York Hilton Midtown while attending an annual investors' meeting. According to reports, Thompson had previously received death threats, and his public profile and scheduled appearance made him a target. The suspect, who was arrested days later, had allegedly stalked Thompson and had knowledge of his travel and appearance schedule. This tragic case represents the most extreme consequence of executive targeting and highlights the life-or-death importance of comprehensive protection, including management of public information about executive whereabouts and activities.

Case 2: Repeated Armed Attacks on Tech CEO's Residence

In a particularly alarming case from 2024, the CEO of an Oregon-based technology company experienced multiple shooting incidents targeting their home. The repeated nature of these attacks demonstrated a determined effort to harm the executive at their residence. Security experts noted that the attacker likely identified the executive's home address through publicly available information, underscoring how digital exposure can enable sustained physical threats.

Case 3: Executive Forced to Flee Home After Online Targeting

In 2022, Twitter's former head of trust and safety, Yoel Roth, was forced to flee his home after facing doxxing and harassment. According to reporting by The Washington Post and CNN, after Elon Musk shared misleading information about Roth's academic background, online users quickly discovered and published his home address. The subsequent threats were severe enough that Roth had to relocate for his safety. This case demonstrates how quickly digital exposure can escalate to physical safety concerns for high-profile executives.

Case 4: "Swatting" Attack on Tech CEO

In 2021, Twitch CEO Emmett Shear was reportedly targeted in a "swatting" attempt—where attackers make false emergency calls to trigger armed police responses at a victim's home. This dangerous form of harassment relies entirely on attackers obtaining an executive's home address, typically from data brokers or public records. Such incidents can lead to potentially life-threatening situations when armed responders arrive expecting a dangerous scenario.

💡 The blending of cyber and physical threats represents a particularly dangerous evolution in executive risk. Digital exposure enables physical targeting, while physical access can facilitate digital compromise.

Cyber Threats from Digital Footprints

Compromised personal data privacy leads to compromised cybersecurity. Exposed personally identifiable information enables sophisticated cyberattacks, such as:

- **Spear phishing with precision:** Attackers craft compelling emails using known details about executives, their assistants, family members, and recent activities
- **Corporate Business Email Compromise (BEC):** The FBI reports BEC schemes have cost businesses over $43 billion globally, often targeting C-Suite email accounts to authorize fraudulent transfers
- **Financial account takeovers:** Exposed credentials from personal accounts frequently provide access to corporate systems due to password reuse (remember: 84% of exposed executive passwords come from personal breaches)
- **Deepfakes with AI-powered impersonation:** Voice cloning technology now requires just a 30-second audio sample to create convincing replicas of executive voices, enabling fraudulent authorizations and directives
- **Social engineering:** Detailed knowledge of executives' backgrounds, interests, and connections enables manipulative attacks that bypass technical security controls

Real-World Cases: High-Profile Digital Attacks on Executives

Case 1: $25 Million Lost in Deepfake CFO Video Call

In January 2024, Hong Kong police reported an unprecedented fraud case where an employee was tricked into transferring $25 million after participating in what appeared to be a legitimate video conference with multiple company executives. According to CNN reporting, the finance worker received messages about a confidential transaction and was then invited to a video meeting that included what appeared to be the company's CFO and other colleagues—all of whom were actually AI-generated deepfakes. This landmark case demonstrates the evolution from earlier voice-cloning attacks to sophisticated video impersonation of multiple executives simultaneously, creating nearly perfect deception that bypassed normal verification procedures.

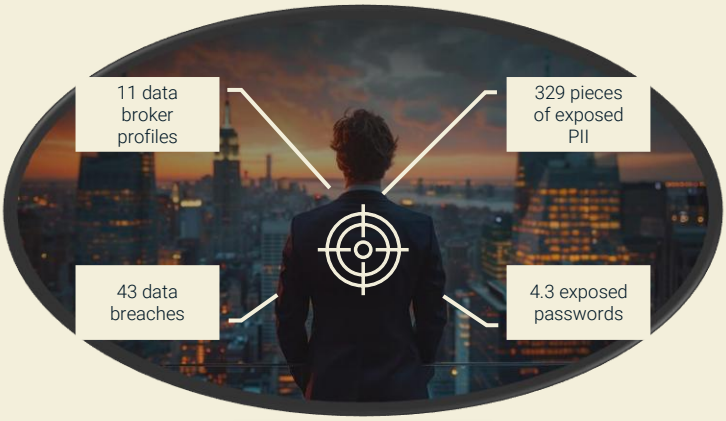
Case 2: LAPSUS$ Group's Executive-Focused Campaign

In 2022, the LAPSUS$ hacking group made headlines by specifically targeting executives at major technology companies including Microsoft, Okta, and NVIDIA. According to Microsoft's Security Blog and official statements from affected companies, the group exploited executives' personal information to conduct highly effective social engineering attacks. They gained access to corporate networks through compromised personal accounts and bypassed multi-factor authentication by targeting executives' personal devices. The FBI noted that the group's success stemmed directly from their exploitation of executives' digital footprints, focusing particularly on exposed credentials and personal contact information.

Case 3: $400,000 Lost in Executive BEC Scam

In 2020, entrepreneur and "Shark Tank" judge Barbara Corcoran lost nearly $400,000 in a sophisticated business email compromise scam. As reported by CNBC and People Magazine, scammers studied Corcoran's digital footprint and business processes, then created a convincing email that appeared to come from her assistant to her bookkeeper. The email requested a payment for a renovation project—a completely plausible request given Corcoran's real estate investments. The scam succeeded because the attackers had accurate information about her business operations, communication patterns, and relationships. Only a last-minute discovery of the scammer's actual email address prevented the full loss.

💡 Compromising executives and their business processes via social engineering, fueled by exposed PII, is the precursor to serious consequences such as financial fraud, data breaches, ransomware attacks, and reputational damage. More than 92% of all cyber attacks exploit human vulnerabilities.

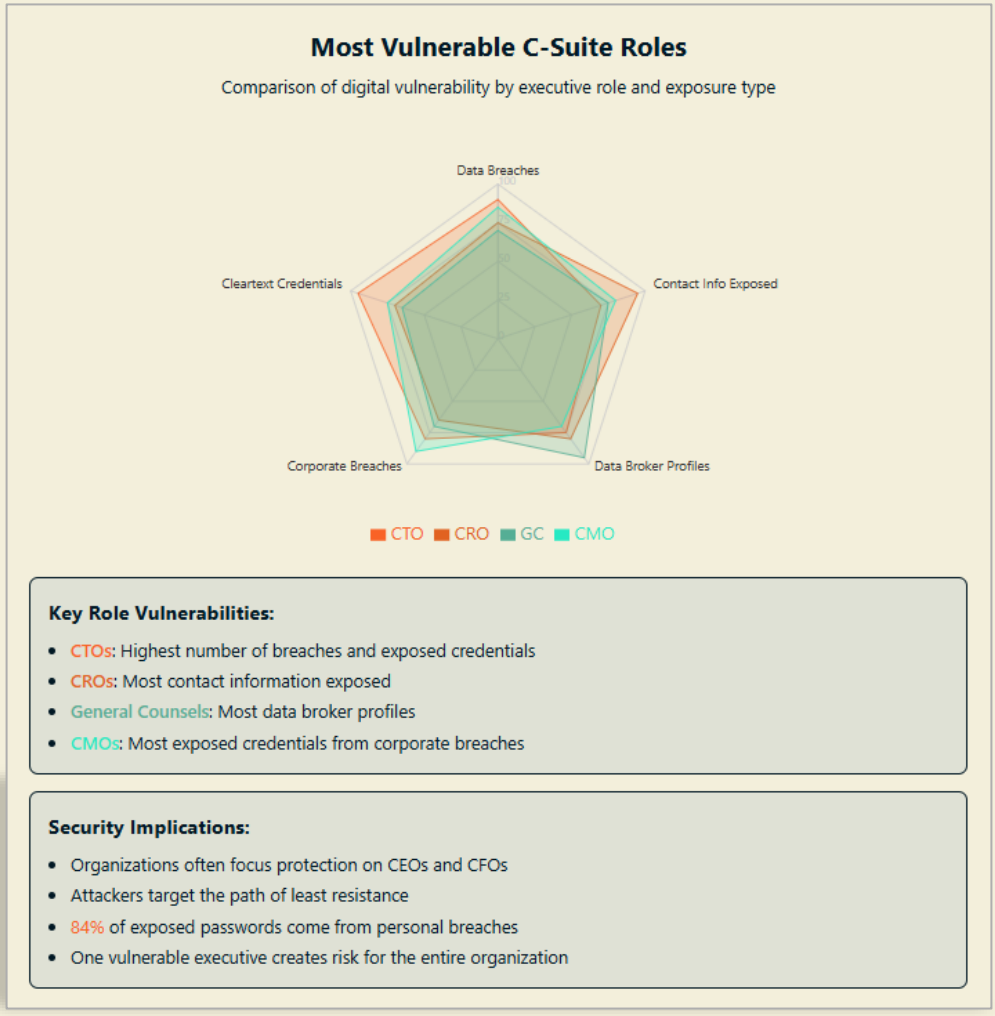


Which Leaders Face the Greatest Risk?

Our analysis of the digital footprint of more than 10,000 C-suite executives in the USA reveals significant variation in digital exposure across roles. While organizations often focus protection efforts on CEOs and CFOs, our data shows attackers have easier paths through other executives. Security is only as strong as its weakest link, and these exposure patterns reveal where those links likely exist in your organization.

Most Exposed Leadership Roles

- **Chief Technology Officers (CTOs):** Highest number of data breaches and exposed credentials. This likely stems from creating numerous accounts throughout their technical careers but poses serious risks given their access to critical systems.
- **Chief Revenue Officers (CROs):** Most contact information exposed, including personal emails and phone numbers. While this accessibility helps in sales roles, it creates significant social engineering vulnerabilities.
- **General Counsels (GCs):** Most data broker profiles make their personal information widely available for purchase. Given their access to sensitive legal and financial information, this creates substantial risk.
- **Chief Marketing Officers (CMOs):** Most exposed credentials from corporate breaches, creating direct access routes to critical marketing systems and data.



Sector-Specific Vulnerability Patterns

Executive exposure varies significantly by industry, with some sectors showing particularly concerning patterns. These industry patterns suggest that different sectors face unique exposure challenges requiring tailored protection approaches.

- **Healthcare:** Healthcare CEOs have the most personal data exposure, including home addresses, personal emails, and dates of birth. The sector also leads in exposed personal phone numbers across all C-level roles.
- **Software:** C-Suite executives face the most personal breaches and highest total breach count, creating substantial risk of credential compromise and account takeover.
- **Government Administration**: Government executives have the most data broker profiles, making their personal information widely available despite heightened security concerns.
- **Information Technology and Services:** IT services leaders show the second-highest personal breach rate and are among the top three most commonly exposed across all credential types.
- **Higher Education:** Academic leadership faces the highest rate of corporate breaches, creating direct attack paths to institutional systems.

Digital Executive Protection: A Framework for Action

Protecting executives requires a comprehensive approach that addresses both the identification and remediation of digital exposure:

Continuous Monitoring and Removal

The Problem: Executive PII constantly spreads across data brokers, breach repositories, and public sources.

The Solution:

- Implement continuous scanning for executive and family PII across all public sources
- Establish automated data broker removal processes that run perpetually
- Monitor breach repositories for newly exposed credentials
- Create alerts for new exposure instances that require immediate attention

Key Metric: Reduce executive PII exposure by at least 90% within 90 days of implementation.

Credential Security Enhancement

The Problem: 94% of executives have exposed plaintext credentials, with an average of 4.3 exposed passwords per leader.

The Solution:

- Identify all exposed executive credentials across breach repositories
- Implement enterprise-wide password management solutions
- Enforce multi-factor authentication for all executive accounts
- Establish credential monitoring to detect new exposures
- Create separate high-security accounts for critical system access

Key Metric: Neutralize 100% of known exposed credentials within 30 days.

Family Protection Integration

The Problem: Attackers increasingly target executive family members as security bypass routes.

The Solution:

- Extend digital footprint monitoring to executive family members
- Remove family PII from data brokers and public sources
- Provide security awareness training for family members
- Establish family communication protocols for security concerns
- Monitor social media for exposure of family information

Key Metric: Reduce family member PII exposure by at least 80% within 90 days.

Privacy Defense

The Problem: Exposed PII enables highly convincing social engineering attacks.

The Solution:

- Conduct regular social engineering testing for executive teams
- Implement enhanced verification protocols for sensitive requests
- Create clear procedures for validating financial and data access requests
- Train executive assistants on social engineering defense tactics
- Develop response plans for voice cloning and deepfake attempts

Key Metric: Achieve ≥90% detection rate on simulated social engineering attempts.

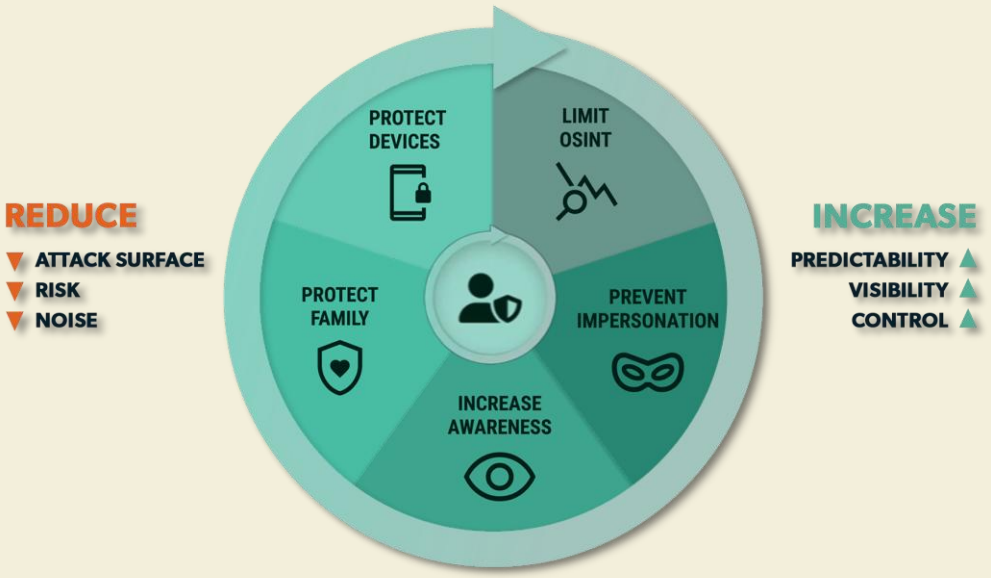
Physical-Digital Security Integration

The Problem: Digital exposure creates physical security risks and vice versa.

The Solution:

- Integrate digital exposure monitoring with physical security operations
- Establish joint response protocols for hybrid threats
- Conduct combined threat assessments across both domains
- Implement travel security measures informed by digital exposure monitoring
- Create unified executive protection dashboards for comprehensive visibility

Key Metric: Conduct monthly cross-team reviews with documented action items.



The VanishID Approach

Comprehensive Digital Executive Protection

VanishID's digital executive protection platform addresses the full spectrum of executive digital exposure risks:

How It Works

Our solution provides:

Comprehensive Digital Footprint Discovery

- Identifies exposed executive and family PII across all public sources
- Maps connections between exposed information elements
- Creates risk-scored exposure profiles for each executive

Continuous Monitoring and Remediation

- Automatically and continuously removes executive and family information from data brokers
- Monitors breach repositories for newly exposed credentials
- Alerts security teams to critical new exposures

Specialized Risk Mitigation

- Neutralizes exposed credentials to prevent unauthorized access
- Reduces public accessibility of executive and family information
- Decreases attack surface for social engineering attempts

Integration with Existing Security Programs

- Provides API-based connections to security infrastructure
- Enables unified dashboards for physical and digital protection
- Delivers actionable intelligence for security operations

Measurable Results

Organizations implementing VanishID's solutions typically see:

- 93% reduction in data broker profiles within 90 days
- 85% decrease in accessible personal information across all sources
- 100% identification of exposed credentials enabling comprehensive remediation
- Significant reduction in targeted phishing attempts against protected executives
- Enhanced physical security posture through reduced address exposure

Key Considerations

Utilizing a consumer-focused service to deliver an enterprise-focused security outcome is a bad choice. When researching and shortlisting vendors to remove executive's PII from the public web, making an initial distinction between consumer and enterprise services is essential. In addition to the features offered by consumer-focused solutions, enterprise-focused solutions comprise the same or similar features offered to individuals, plus many more tailored to the needs of security teams. On the other hand, consumer-focused services may also include additional features irrelevant to enterprise privacy and security (i.e., identity theft insurance, credit monitoring, ad blockers, etc).

Consumer-grade services often:

- Offshore PII removal tasks and share PII with 3rd parties
- Manually perform data broker takedowns, a process that is not continuous
- Require effort from customers
- Do not provide insights at the enterprise level
- Overstate the problem and lack transparency (i.e., you have 600 profiles -- false!)

To help select the most appropriate type of digital executive protection service, we've produced a Guide for Choosing the Right PII Removal Service for your Business, where we go deep into what to consider to avoid pitfalls.

Taking Action

Next Steps for Security Leaders

Your executive team's digital exposure isn't hypothetical—it's a proven reality affecting nearly every C-suite member. The data is clear: 93% have exposed home addresses, 94% have leaked passwords, and virtually all have been caught in data breaches. The question isn't if your leadership is vulnerable but how you'll protect them.

The 2024 assassination of UnitedHealthcare CEO Brian Thompson—targeted at a public event—starkly illustrates the fatal risks of inadequate protection. In its aftermath, requests for executive security services surged as companies confronted this new reality.

Here's how to get started:

1. **Assess your current exposure:** Request a complimentary digital exposure assessment for your executive team
2. **Review your existing protection measures:** Evaluate how your current security programs address digital footprint risks
3. **Develop an integrated protection strategy:** Create a comprehensive approach that spans both physical and digital domains
4. **Implement continuous monitoring and remediation:** Deploy solutions that provide ongoing protection against new exposures
5. **Measure and report on risk reduction:** Track concrete metrics showing decreased executive vulnerability

The convergence of digital and physical security risks demands a unified approach to executive protection. By implementing comprehensive digital executive protection, you not only protect your leadership team but strengthen your organization's overall security posture.

For a complimentary digital exposure assessment of your executive team, contact VanishID at www.vanishid.com/demo.

VanishID

7315 Wisconsin Ave
Suite 400W
Bethesda, MD, 20814

Follow us on