RAPID7

THREAT REPORT

# EXECUTIVES' DIGITAL FOOTPRINTS: THE OVERLOOKED CORPORATE VULNERABILITY

Rapid7 Labs

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

The digital exposure of high-ranking corporate personnel through social media activity, professional profiles, and metadata represents a growing threat vector in the cybersecurity landscape.

Threat actors increasingly exploit these digital footprints to conduct targeted campaigns, such as business email compromise (BEC) scams, spear phishing, credential harvesting, and hybrid cyber-physical attacks.

What begins as open-source intelligence (OSINT) gathering can quickly escalate into operationalized threats.

Social engineering is one of the most effective techniques in the attacker's toolkit because it targets human vulnerabilities. Adversaries routinely scrape social platforms, correlate breached data, and perform targeted reconnaissance on executives and other high-value individuals. This intelligence fuels tailored attack paths that often bypass traditional security controls, putting the individual and the enterprise at risk.

For organizations, this convergence demands a shift toward intelligence-driven defense strategies. Monitoring executive digital footprints, deploying real-time threat detection, and integrating physical security with cyber intelligence are no longer optional; these are essential components of modern risk management.

# CORPORATE EXECUTIVES IN THE CROSSHAIRS

## Threat actor motivations

The elevated online visibility of a company's executives presents a substantial cybersecurity vulnerability. Their extensive digital footprint — encompassing professional profiles, public statements, and personal social media — serves as an invaluable intelligence source for malicious actors. This exposure renders executives prime targets for advanced persistent threats, including sophisticated phishing attacks, impersonation schemes, and the emerging threat of AI deepfakes.

A successful compromise of an executive's digital account extends beyond individual privacy concerns. It can directly facilitate unauthorized access to sensitive corporate data, instigate financial fraud, and inflict severe reputational damage, critically undermining the organization's overall security posture.

## Targeted information

As can be expected, the most accessible information forms the foundation of an attacker's research. An executive's digital life, scattered across social media, public records, and general web results, creates a detailed and exploitable profile. This publicly-available data is the entry point for most targeted threats (Figure 1).

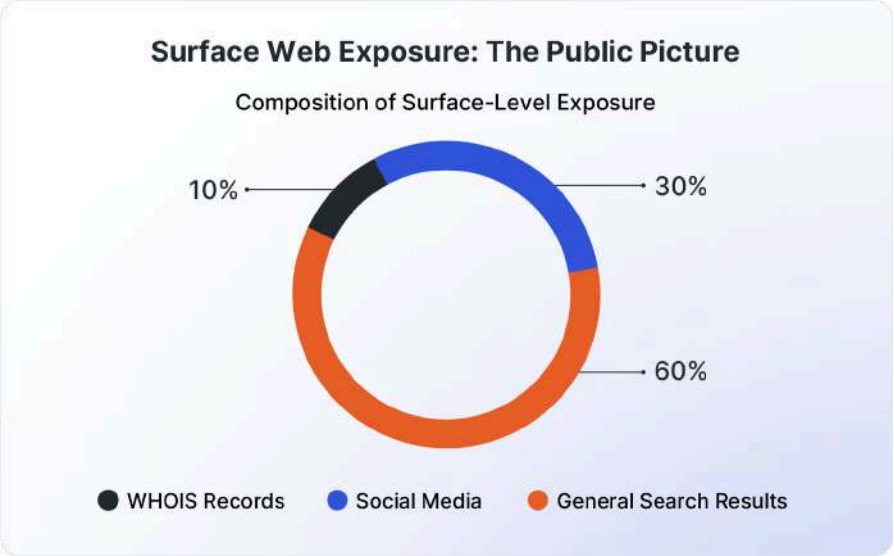


Figure 1: Composition of surface-level web exposure

Today, 60% of an individual's digital risk exposure is easily retrievable through a general search on the surface web. This publicly-available information includes public records, videos, and articles, as well as details like educational and career histories, and even signatures. Such seemingly innocuous information, when pieced together, can be exploited in various cyber scams, including business email compromise, phishing attacks, and impersonation attempts, posing a direct threat to organizational security.

**Public records** represent a significant and accessible vulnerability for executives and their companies. Information like property deeds, voter registrations, business licenses, and official company appointments can be easily found and aggregated. This data fuels Open-Source Intelligence activities, allowing malicious actors to construct detailed profiles containing physical addresses, family connections, financial assets, and personal routines. This deep insight enables highly targeted threats such as doxxing, physical harassment or stalking, extortion, and sophisticated impersonation schemes. Worst-case outcomes can involve serious compromises to the target executive's (and even their family's) safety, damage to the company's reputation, and critical security vulnerabilities.

**Social media** exposure also presents significant risks for executives and their companies. The inadvertent sharing of personal details creates vectors for attackers to employ sophisticated social engineering techniques.

This includes crafting highly convincing phishing campaigns, orchestrating BEC scams by impersonating the executive, or even attempting account takeovers by using publicly available information to bypass security questions. Such successful attacks can lead to severe data breaches, substantial financial losses for the company, and widespread damage to its reputation and trustworthiness.

A prime example of this risk unfolded in 2023 during the MGM Resorts cyberattack, where the Scattered Spider threat group leveraged details harvested from the LinkedIn of an MGM employee to cripple the company's operations. By identifying the employee's name, role, and professional connections on the platform, an attacker was able to call the company's IT help desk and convincingly impersonate that individual. Claiming to have lost access to their credentials, the attacker used the "scraped" personal details to bypass security verification, gaining the administrative access necessary to deploy ransomware. This single point of

failure, rooted in publicly accessible social media data, resulted in a $100 million financial loss and widespread operational chaos, illustrating how a professional profile can inadvertently serve as a blueprint for a catastrophic breach.

## Leaked credentials

Leaked credentials refer to compromised authentication data, such as usernames, passwords, API keys, or authentication tokens that become exposed through data breaches, malware infections, phishing campaigns, or third-party compromises. Once leaked, these credentials often circulate on underground forums, dark web marketplaces, or automated attack toolkits, significantly lowering the barrier to entry for malicious actors.

Because credentials are the primary mechanism for identity and access management, their exposure effectively bypasses many security controls, enabling attackers to operate as legitimate users. The consequences extend far beyond a single account compromise, frequently cascading across interconnected systems, organizations, and supply chains. The risks associated with leaked credentials are therefore systemic, persistent, and highly exploitable. They include the following:

- **Account takeover (ATO):** Attackers can directly access user, corporate, or administrative accounts, leading to loss of control over systems and services.
- **Credential stuffing and lateral movement:** Reused passwords allow attackers to compromise multiple platforms and escalate privileges across interconnected systems.
- **Operational disruption:** Compromised accounts may be used to deploy malware, ransomware, or sabotage critical business operations.
- **Data exfiltration and espionage:** Sensitive personal, corporate, or classified information can be stolen, sold, or exploited for intelligence-gathering purposes.
- **Social engineering and identity theft:** Leaked credentials can be leveraged to craft highly targeted phishing, impersonation, or identity fraud campaigns as a means of collecting additional credentials and sensitive data.

- **Financial loss and fraud:** Unauthorized access may result in fraudulent transactions, theft of funds, or misuse of payment information.
- **Long-term persistent threats:** Stolen credentials can remain usable for extended periods, enabling repeated or delayed attacks even after the initial breach.

# RESEARCH METHODOLOGY

Over the last several years, Rapid7 has worked with hundreds of corporate executives representing organizations around the world and spanning roles such as Founder, President, CEO, CFO, CISO, etc., to understand and reduce their digital risk. A comprehensive look at the data from Rapid7's 2024 and 2025 engagements shows us overall areas for improvement in executives' digital footprints.

Rapid7 has developed a unique metric that we call the Rapid7 Exposure Prevention (REP) Score. The REP Score provides a clear, quantitative assessment of an individual's total online exposure by averaging the risk calculated across 4 key areas: general exposure, social media, public records, and leaked credentials.

Like grading on a test, a REP Score of 0% indicates total exposure, while 100% signifies no exposure whatsoever, giving you an immediate understanding of an executive's digital risk level.

# EXECUTIVE DATA EXPOSURE BY INDUSTRY

To identify trends and patterns based upon specific industries, we analyzed data from each of the 3 components within its respective Global Industry Classification Standard (GICS) sectors.

There is a noticeable difference in total exposure among sectors, with Industrials having the lowest total exposure and Consumer Discretionary (i.e., non-essential consumer goods) having the highest.

- **Lowest exposure:** Industrials perform best with a total exposure score of 73.04%, indicating a lower overall vulnerability or presence across the analyzed categories.
- **Highest exposure:** Consumer Discretionary has the worst total exposure score at 63.98%, suggesting a comparatively higher overall risk profile in this area.
- **Average total exposure:** The average total exposure score across all sectors is approximately 69.04%.

Social Media and Public Records consistently show high exposure percentages across most sectors, highlighting them as less prone to data exposure.

Leaked credentials consistently show high exposure percentages across most sectors, highlighting them as prominent channels for data exposure, with Information Technology having the best score and Real Estate the lowest score.

- **Real Estate's vulnerability:** Real Estate has the highest leaked credentials exposure at 32%, suggesting a relatively increased vulnerability in this area compared to other sectors.
- **Average leaked credentials exposure:** The average exposure from leaked credentials across all sectors is 51.27%.

# COMPARING U.S. AND EUROPEAN EXECUTIVES

To better understand the nuances and fundamental differences between organizational approaches in Europe and the U.S., we conducted a comprehensive and in-depth comparison. This analysis aimed to identify key disparities in management styles, corporate culture, regulatory frameworks, and employee relations, providing a more holistic perspective on how these two distinct regions operate within the global business landscape.

The comparison was made according to the REP index's different sub-categories: General Exposure, Social Media, Public Records, Leaked Credentials, and Total.


## General exposure

Analyzing the average "General Exposure" for executives in the U.S. and Europe reveals a nuanced difference between the two regions. This small difference might be perceived as counterintuitive considering distinct privacy laws like the General Data Protection Regulation (GDPR) and varied cultural and social norms; however, it seems that several structural and technological forces have bridged the gap between these two regions, leading to a phenomenon known as Media Convergence. Individuals in both regions seek professional branding using nearly identical technologies, even at the expense of their online privacy. In addition, the rise of global freelance and creator economies means individuals in both regions must "market" themselves online to remain competitive, leading to similar levels of self-disclosure and public visibility.

## Social media

The Social Media section also manifests subtle differences between the regions, likely for similar reasons. However, we do see that European executives are slightly more exposed than their U.S. counterparts. This might be explained by cultural and social variables, such as higher trust in public institutions and regulators in Europe compared to the U.S., reduced fear of political or social retaliation, and less anxiety about public exposure.

## Public records

In this section of our research, we can see significant differences between U.S. and European executives, with U.S. individuals being more exposed in this domain (having lower REP scores). These differences might be explained by:

- **GDPR and Data Privacy (Europe):** The General Data Protection Regulation in Europe imposes strict rules on data privacy and the use of personal information. This can make companies and executives more cautious about the amount of personal information shared online, including professional profiles. While not directly preventing online presence, it can influence the nature and extent of it.
- **Fewer Restrictions (U.S.):** While data privacy concerns exist in the U.S., the regulatory landscape has historically been less stringent than GDPR, potentially leading to a more relaxed approach to online data sharing.

## Leaked credentials

Based on our data, the executives in Europe face a lower exposure of their digital access details compared to executives in the U.S. (having higher REP scores). This is likely to be primarily driven by the higher focus many threat actors give to U.S. companies, leading to more frequent breaches. Another factor is that GDPR fines and proactive scrutiny are more intense than the reactive measures in the U.S., potentially leading to better customer data protection.

## Total data exposure

Overall, the analysis shows that U.S. executives are slightly more digitally exposed than their European counterparts. Despite nuanced differences in the General Exposure and Social Media sections, U.S. executives showed significantly higher exposure levels in terms of public records and leaked credentials, likely due to reasons mentioned earlier, such as GDPR and E.U. privacy protective rules, as well as the prolific malicious activity targeting the U.S.

# RECOMMENDATIONS

Security teams can help their organization's executives make simple changes to significantly reduce the risks they face online. The following are recommendations for protecting both executives and the companies they represent.

## Shrink digital exposure

Reducing an executive's digital exposure begins with minimizing their online presence. The organization should encourage executives to limit real-time location updates or excessive personal details on social media. What seems harmless can be pieced together by bad actors. This is what the executive should do:

- Lock down social media privacy settings to the strictest level.
- Remove unnecessary personal info from company websites and public bios.
- Opt out of data broker sites (e.g., WhitePages, Spokeo) that sell personal data. This is ongoing, so regular checks are key.
- Delete old, inactive online accounts that are no longer in use.

## Boost the security shield

Strong passwords and Multi-Factor Authentication (MFA) are non-negotiable. Mandate unique, complex passwords for all accounts. Use password managers and enable MFA on everything, especially email and financial apps. Authenticator apps or hardware keys are better than SMS for MFA.

Secure all devices and networks. Keep devices and software updated. Use an antivirus, and always use a VPN on public Wi-Fi. Privacy screens for laptops in public are smart, too.

Finally, help the executive sharpen their phishing radar. Provide regular training on identifying phishing, spear-phishing, and social engineering. Teach them to always verify suspicious requests through a separate, trusted channel.

### Monitor and respond

Set up continuous monitoring of the executive's digital assets. Use digital risk protection tools to scan the web for exposed credentials or impersonation attempts. Get real-time alerts for any suspicious activity.

Have a plan. Develop a clear incident response plan for digital breaches. Know what to do if an executive's account is compromised: how to lock it down, wipe devices, and communicate with stakeholders.

## CONCLUSION

The findings discussed within this research report underscore that executives' digital footprints are not merely a privacy issue but a critical and often overlooked corporate vulnerability. Our analysis, quantified by the Rapid7 Exposure Prevention Score, demonstrates a measurable and varied risk across industries and geographies, with public records and leaked credentials consistently emerging as primary exposure vectors. The observed disparities, such as the lower public records exposure in Europe, likely influenced by GDPR, highlight the complexity of this threat landscape.

Passive OSINT gathering can rapidly escalate and become operationalized into advanced BEC and spear-phishing campaigns, or even hybrid cyber-physical attacks. To mitigate this risk, a strategic, intelligence-driven defense is essential. This requires a comprehensive program that limits the executive's digital risk with strong authentication protocols, continuous digital asset monitoring, and a detailed incident response plan.

By making the proactive, defensive, and reactive components of modern risk management non-negotiable, organizations can effectively protect their high-value personnel and, by extension, secure the entire enterprise from escalating digital and physical threats.

## ABOUT RAPID7

Rapid7, Inc. (NASDAQ: RPD) is a global leader in AI-powered managed cybersecurity operations, trusted to advance organizations' cyber resilience. Open and extensible, the Rapid7 Command Platform integrates security data, enriching it with AI, threat intelligence, and 25 years of expertise and innovation to reduce risk and disrupt attackers. As a recognized leader in preemptive managed detection and response (MDR), Rapid7 unifies exposure and detection to transform the cybersecurity operations of more than 11,500 customers worldwide. For more information, visit our website, check out our blog, or follow us on LinkedIn or X.