SOCRadar®
Your Eyes Beyond

Whitepaper

Executive Digital Protection:
Why Your C-Suite Is the Most Exposed Asset in Your Organization

Contents

Executive Summary

Cybercriminals are targeting senior executives with increasing precision and success. Business email compromise (BEC) alone cost organizations $3.04 billion in 2025, according to the FBI, and 63% of organizations reported experiencing at least one BEC attack during the year. The total cost of cybercrime reported to the FBI reached $20.8 billion, a 26% increase from the prior year.

Meanwhile, attackers have access to a new generation of tools. AI-generated deepfakes have already been used to impersonate CFOs on video calls, clone CEO voices from public recordings, and fabricate entire virtual meetings with multiple fake executives.

Executives carry outsized digital risk because they have outsized access, visibility, and authority. Their credentials appear on the dark web at high rates, their public profiles give attackers material for social engineering, and their decisions can move millions of dollars with a single authorization. Despite this, most organizations provide no additional cyber protection for their leadership.

SOCRadar's VIP Protection module addresses this issue by providing continuous monitoring of executive digital identities, detecting credential exposures, PII leaks, and impersonation attempts before they can be weaponized.

> *SOCRadar's VIP Protection module addresses this gap by providing continuous monitoring of executive digital identities, detecting credential exposures, PII leaks, and impersonation attempts before they can be weaponized.*

The Threat Landscape

The scale of cybercrime targeting businesses has grown every year for the past decade, but the acceleration in 2024 and 2025 especially stands out. We assess that three shifts define the current environment.

Cybercrime by the Numbers
The FBI's Internet Crime Complaint Center received over one million complaints in 2025, with total reported losses of $20.8 billion and BEC was the second-highest loss category. Roughly 86% of BEC funds moved through wire transfers or ACH, meaning the money left the victim's control almost immediately.

For the first time, the FBI formally tracked AI-related cybercrime as a distinct category. As a result, they state 22,364 complaints and $893 million in confirmed losses. Additionally, these figures are likely a significant undercount, since many victims do not realize AI was involved in the attack they experienced.

The Human Element Remains Central
In the Verizon 2026 Data Breach Investigations Report 31,000 incidents were analyzed and it was found that the most frequent breach causes continue to heavily involve the human element: social engineering, phishing, and stolen credentials.

Mobile-based social engineering, including voice and text-based scams, achieved a 40% higher click-through rate than traditional email phishing in simulations. It is important because executives are often targeted through personal devices and channels outside corporate email filters. The DBIR also documented that pretexting, where attackers fabricate a scenario or identity to manipulate a target, has become one of the top initial access methods, driven in large part by AI capabilities.

AI as a Force Multiplier
SOCRadar's AI Threat Landscape Report found that AI is no longer an enhancement to criminal operations but an operational layer embedded across every phase of the attack chain, from reconnaissance to monetization. In documented sessions, AI voice agents extracted credentials while the human operator never spoke a word.

How SOCRadar Addresses This Threat Landscape

An effective executive protection program goes beyond standard enterprise security. It addresses the specific ways executives are targeted and provides capabilities tailored to their unique risk profile.

Continuous Dark Web Monitoring

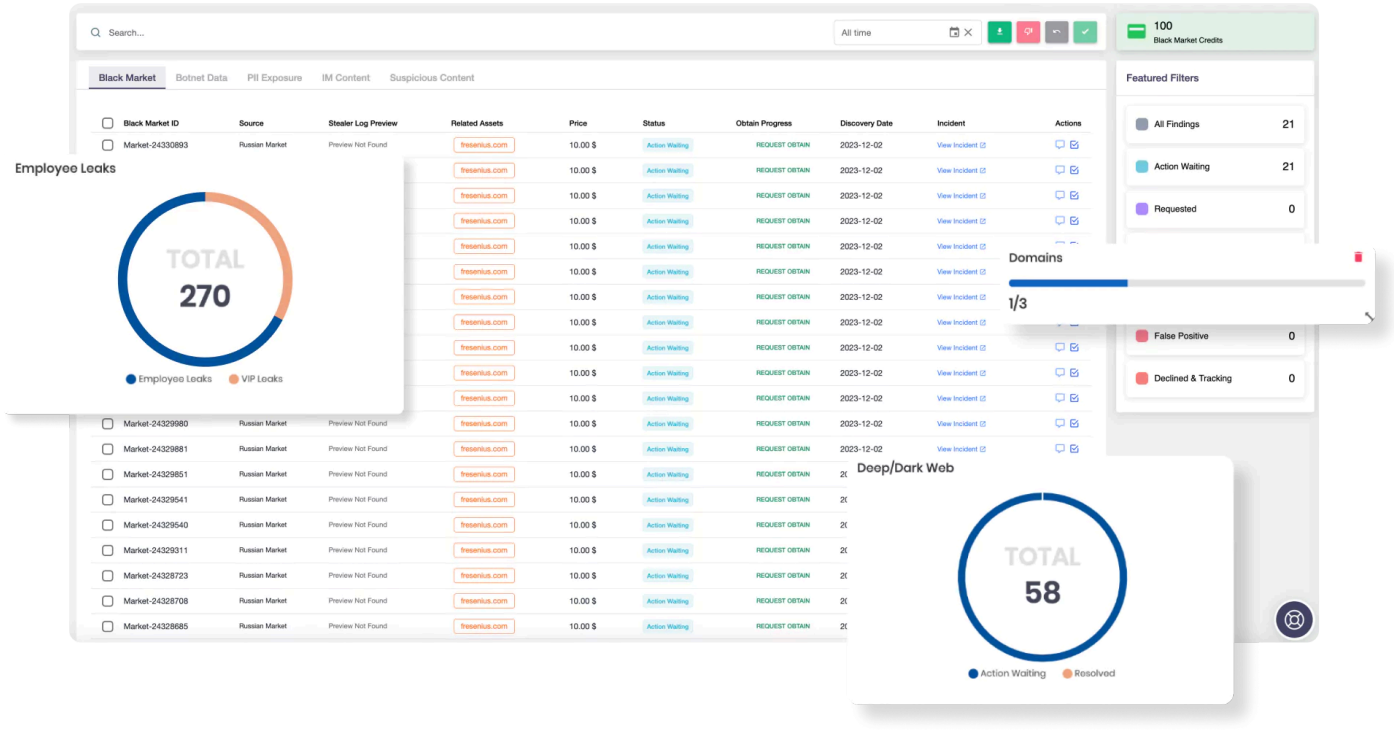
Security teams need ongoing visibility into whether executive credentials, personal data, or sensitive corporate information has appeared on the dark web. This includes monitoring hacker forums, Telegram channels, Dark Web marketplaces, paste sites, and underground data brokers.

Credential and Breach Exposure Tracking

Every executive's personal and professional email addresses should be continuously checked against known breach databases and infostealer log compilations. When a match is found, the response should be immediate: password rotation, session revocation, and investigation of any account activity during the exposure window. This capability should extend beyond corporate email to cover personal accounts that executives may use for work-related communication.

PII and Financial Data Surveillance

Monitoring should cover personally identifiable information (social security numbers, home addresses, phone numbers) and financial data (credit card numbers, bank account details) belonging to executives. When this data surfaces on underground markets or in breach dumps, the organization needs to know immediately so it can initiate identity protection measures, fraud alerts, and, where applicable, law enforcement engagement.



Executive Impersonation Detection

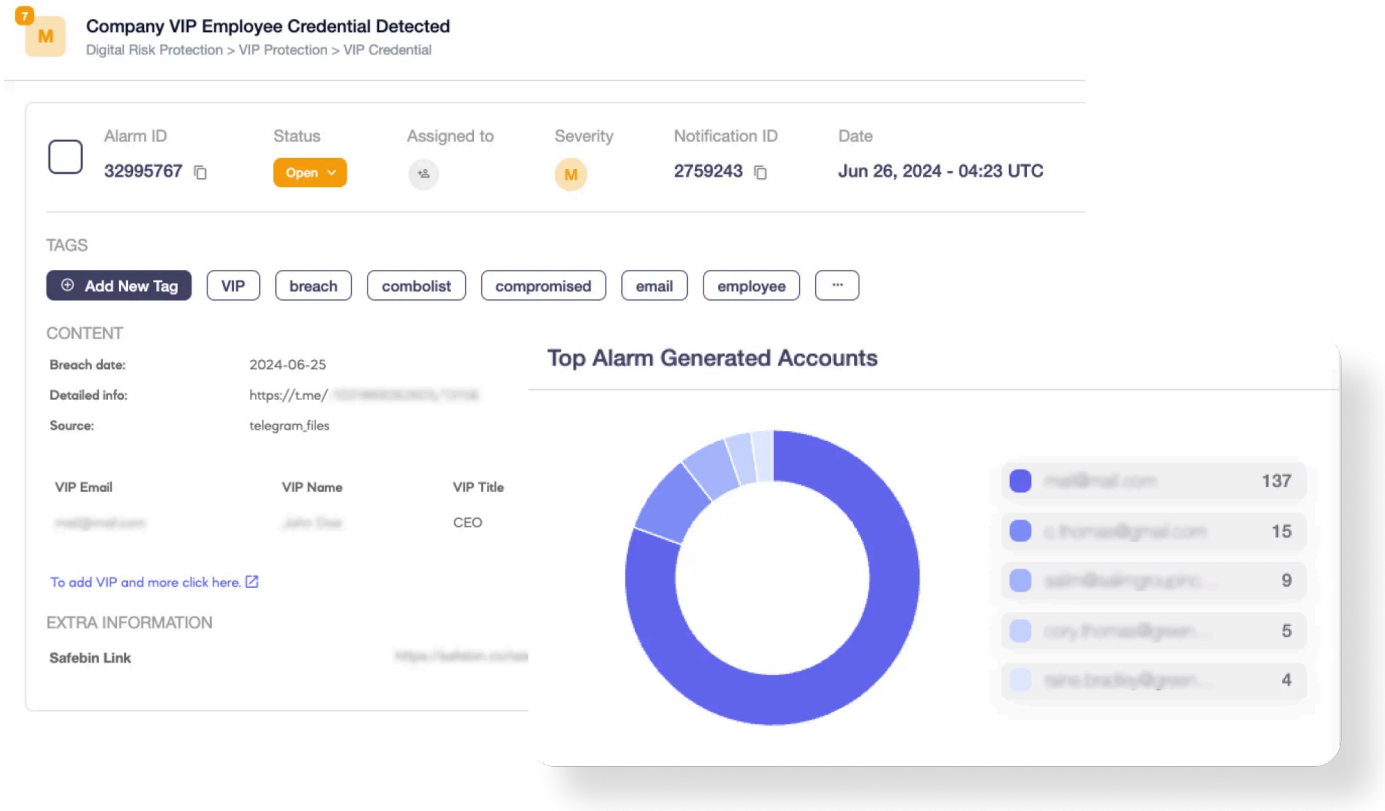
Attackers routinely create fake social media profiles, lookalike domains, and fraudulent websites using executives' names and photos. A comprehensive protection program should continuously scan for these impersonation attempts and provide or facilitate rapid takedown capabilities.

Real-Time Alerting and Customized Thresholds

Each executive faces a different threat profile based on their role, public visibility, industry, and geographic exposure. Monitoring and alerting should be customized per individual, with thresholds calibrated to their specific risk factors. A tailored system will deliver actionable intelligence that security teams can respond to quickly.

Takedown and Remediation Workflows

Detection is only valuable if the organization can act on it. The protection program should include established workflows for taking down fraudulent domains, fake social media accounts, and impersonation sites.



How Attacks on Executives Unfold

Attacks targeting executives follow recognizable patterns. Understanding these patterns is the first step toward building defenses that work.

Deepfake Video and Voice Impersonation

One of the most dramatic evolutions in executive-targeted attacks is the use of AI-generated deepfakes to impersonate senior leaders in real time.

The Arup case (Hong Kong, 2024). A finance employee at multinational engineering firm Arup received an email from someone claiming to be the company's UK-based CFO, requesting a series of confidential transactions. The employee was initially suspicious and requested a video call to verify. On the call, the CFO and several other senior colleagues appeared on screen. Every participant looked and sounded authentic. The employee proceeded to make 15 transactions totaling $25 million to five bank accounts. All participants on the call were AI-generated deepfakes. The fraud was only discovered when the employee later checked with the head office.

The Singapore case (March 2025). A finance director at a separate multinational firm joined what appeared to be a routine Zoom call with senior leadership. Every face was a deepfake, every voice was AI-generated. The finance director authorized a $499,000 transfer before the deception was uncovered.

Ferrari (July 2024): Attackers attempted to impersonate Ferrari CEO Benedetto Vigna using deepfake technology to deceive finance executives. In this case, the targeted executive grew suspicious and the attempt failed.

Wiz (late 2024): Attackers cloned the voice of Wiz CEO Assaf Rappaport from a public conference recording and sent deepfake voicemails to dozens of employees requesting credentials. The attempt failed because the CEO's public speaking voice differed from his everyday conversational tone, and employees flagged the discrepancy.

Business Email Compromise and CEO Fraud

BEC remains the highest-volume financial threat to executives. In 2025, BEC was the case across 24,768 incidents.

The typical BEC scenario involves an attacker gaining access to or spoofing an executive's email account and using it to authorize a fraudulent wire transfer. AI has raised the stakes here as well. The FBI documented cases where AI was used to draft emails that perfectly matched a CEO's writing style, while voice cloning provided phone confirmation that matched the spoofed sender.

Human detection fails when the email looks right and the voice on the phone matches.

Executive Identity Fraud and Impersonation

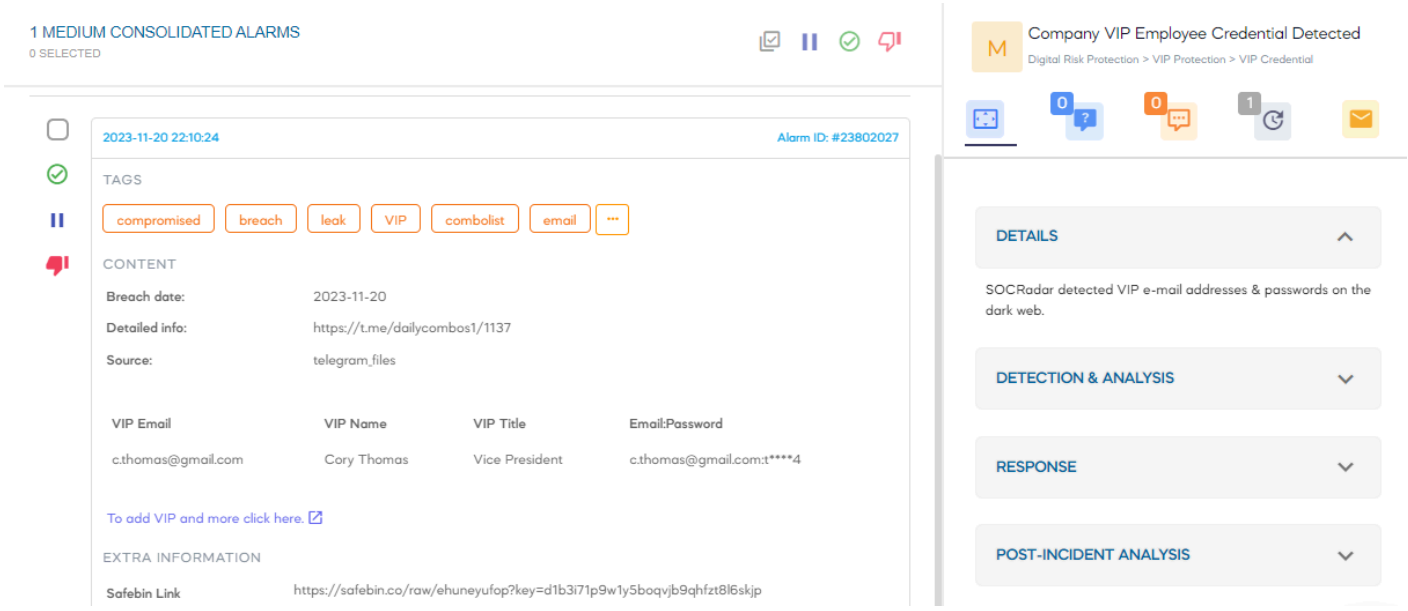
Beyond direct cyberattacks, executives face identity fraud at scale as well. Research indicates that 54% of U.S. companies have reported executive identity fraud. Attackers create fake social media profiles using an executive's name and photo, register lookalike domains, and set up fraudulent websites to deceive employees, partners, and customers.

A common pattern involves creating a convincing fake LinkedIn or WhatsApp profile of a CEO or CFO, then using it to contact employees or suppliers with urgent payment requests. Because the requests appear to come from a known authority figure, they often succeed even when the target has received security awareness training.

Credential Exposure and Dark Web Trading

Over 15 billion stolen credentials currently circulate on the Dark Web and unfortunately organizations whose credentials appear in these markets face a bigger breach risk of those without exposure.

In this market, executive credentials are premium. When an attacker obtains a C-suite login, they gain access to sensitive communications, financial authorization workflows, and strategic information that can be leveraged for further attacks. We can state that credential exposure is one of the most reliable predictor of future account compromise.



Business Impact and Cost of Inaction

The financial costs of attacks on executives are substantial and well-documented but the damage extends beyond the immediate loss of funds.

Direct Financial Loss

When an executive is successfully targeted, the financial damage is severe and immediate. Fraudulent transfers authorized through deepfake impersonation or compromised accounts can drain millions before anyone realizes what happened. Recovery rates are low because most funds leave the organization's control within minutes. It is possible that these costs will accelerate as AI lowers the barrier for attackers.

Reputational Damage

When an executive is impersonated or an organization falls victim to a deepfake-enabled fraud, the reputational cost compounds the financial one. Public disclosure of a major fraud event can erode customer confidence, weaken investor trust, and create lasting brand damage. In some cases, the reputational harm exceeds the dollar value of the fraud itself.

Operational Disruption

A compromised executive account can force an organization into emergency response mode. We are talking about activities like freezing financial workflows, resetting credentials across the organization, conducting forensic investigations, and notifying regulators and partners. These disruptions pull security teams, legal departments, and senior leadership away from their core work for weeks or months.

Regulatory and Legal Exposure

Regulatory expectations are rising. The FBI's explicit public warnings about deepfake fraud, combined with the documented frequency and dollar value of these attacks, mean that organizations can no longer credibly claim they were unaware of the threat. In the event of a successful attack, regulators will examine whether the organization had adequate, documented controls in place at the time. The absence of an executive protection program may itself become a liability.

Implementation Considerations

Building an executive digital protection program requires coordination across security, legal, communications, and executive leadership.

Start with an Exposure Assessment

Before deploying monitoring tools, conduct a baseline assessment of your executives' current digital exposure. Search for their credentials in known breach databases. Check whether their personal information is publicly available or for sale. Identify existing fake profiles or impersonation domains. This assessment establishes the starting point.

Define the Protection Scope

Decide which individuals fall within the program. At a minimum, this should include the CEO, CFO, CTO, CISO, General Counsel, and board members. Depending on the organization's risk profile and industry, it may extend to other senior leaders, heads of business units, or various individuals. The scope should be reviewed regularly as roles change and new threat patterns emerge.

Integrate with Existing Security Operations

Executive protection should not operate in isolation. Alerts from executive monitoring need to feed into SOC or incident response teams. Credential exposures should trigger the same workflows as any other compromised account, with the additional urgency that executive access warrants.

Address the Personal Attack Surface

Personal email accounts, home Wi-Fi networks, personal devices, and family members' social media profiles all represent potential entry points. An effective program acknowledges this reality and provides guidance, and where appropriate, monitoring for the personal digital lives of protected individuals. This requires sensitivity and clear communication about privacy boundaries.

Establish Executive Buy-In

The program will not succeed without active participation from the executives it protects. They need to understand the threat, cooperate with monitoring setup, and follow the response protocols that the program establishes. Frame the program around their personal safety and the organization's financial exposure rather than as a compliance exercise.

Common Pitfalls

The most common failure mode is treating executive protection as a one-time project rather than a continuous program. Threats evolve, new credentials are leaked, and new impersonation attempts appear constantly. A second pitfall is over-relying on training alone. Even well-trained employees are vulnerable to AI-enhanced social engineering. Training is necessary but not sufficient. A third pitfall is limiting monitoring to the corporate domain without covering personal email addresses and social media accounts, which are often the primary attack surface.

Conclusion and Next Steps

Executives are targeted at higher rates than the general employee population, with higher-value attack methods, for higher-stakes payoffs. The data leaves little room for ambiguity on this issue.

The tools available to attackers have advanced significantly in the past years. AI-generated deepfakes can now impersonate executives in real-time video calls, voice cloning can replicate a CEO's speech patterns from a single public recording, and massive credential compilations ensure that most executives have at least some personal data circulating in criminal markets.

At the same time, there are still organizations that provide no additional cybersecurity protection for their executives. This gap between the threat and the response represents significant and avoidable risk.

An executive digital protection program addresses this gap through continuous monitoring, tailored alerting, rapid response capabilities, and integration with broader security operations. The investment is modest relative to the potential losses.

The recommended next steps are straightforward:

1. Conduct a baseline exposure assessment for all C-suite executives and board members.
2. Evaluate and deploy a continuous executive monitoring solution covering dark web, breach databases, social media, and domain impersonation.
3. Integrate executive protection alerts with existing SOC and incident response workflows.
4. Update fraud prevention procedures to account for deepfake voice and video impersonation, including multi-person authorization for high-value transactions.
5. Review and reassess the program quarterly as the threat landscape evolves.

The organizations that act now will be ahead of both the threat and the regulatory curve. Those that wait will find themselves explaining to boards, regulators, and stakeholders why protections were not in place when a documented, foreseeable risk materialized.

How can SOCRadar help your organization?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: "Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services." SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Start free trial

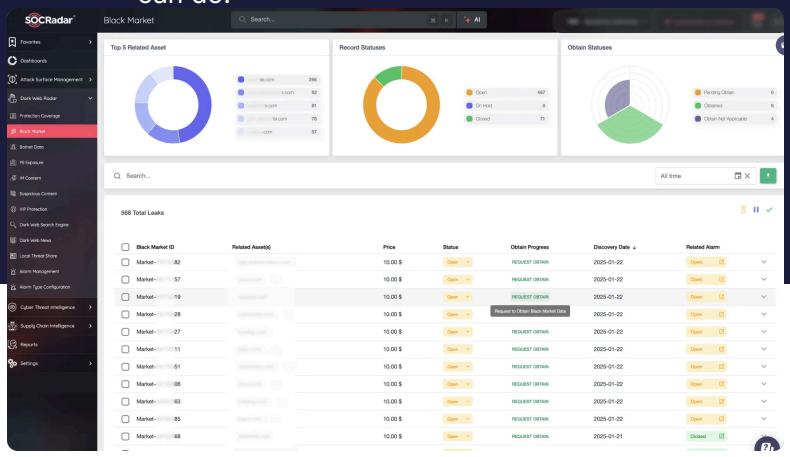
Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.



SOCRadar®
Your Eyes Beyond

socradar.io