

Safeguard Your C-Suite with Executive Digital Protection

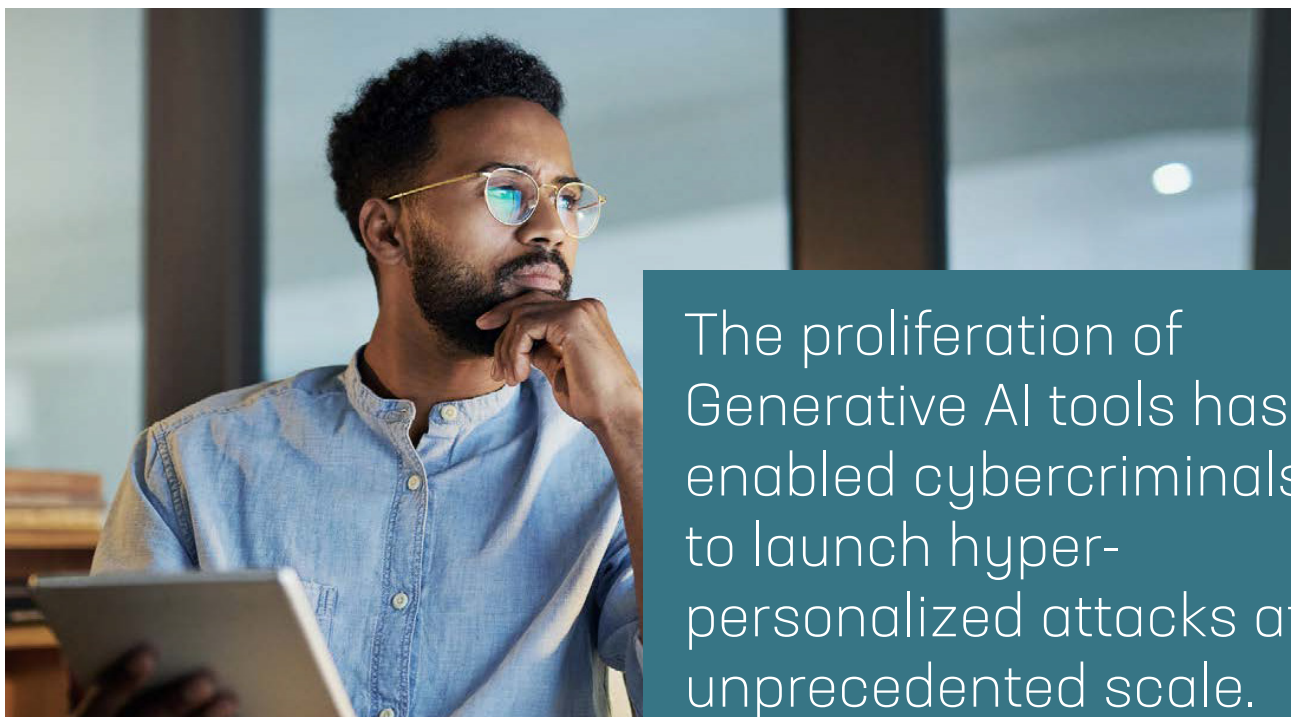
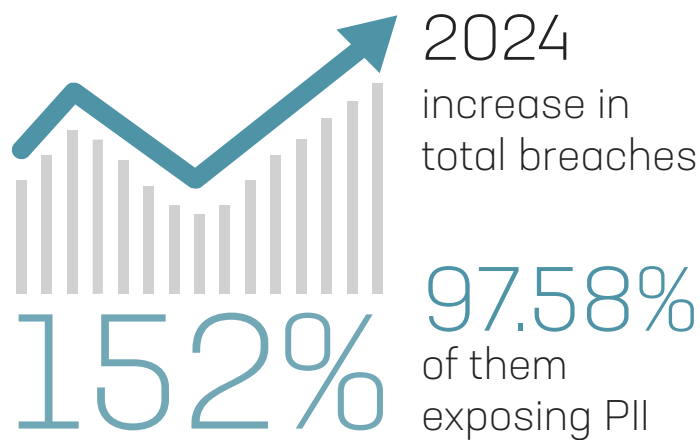


Executive Summary

Executives and high net worth (HNW) individuals face unprecedented threats, from physical harm to burglary to ransomware and other cyber threats, making digital executive protection a business-critical priority. The reliance on remote communication, cloud-based collaboration, and social media presence has expanded executives' digital footprints, increasing their exposure to targeted attacks. In addition, the digital information available makes protecting your most valuable assets as challenging as ever! Today, an executive's cyber life pattern is an extension of their real-world life and the company's reputation. Understanding and mitigating digital risks—both from open web sources and underground cybercriminal networks—is crucial to safeguarding corporate leadership and brand integrity.

***Constella's 2024 Identity Breach Report highlights a 152% increase in total breaches, with 97.58% of them exposing personally identifiable information (PII) - a 39% jump from the previous year.**

The proliferation of Generative AI (GenAI) tools like FraudGPT and WormGPT has enabled cybercriminals to launch hyper-personalized phishing scams, impersonation attacks, and deepfake-based fraud at unprecedented scale. The risk to executives has never been higher, as cybercriminals view corporate leaders as high-value entry points into an organization's sensitive data.



The proliferation of Generative AI tools has enabled cybercriminals to launch hyper-personalized attacks at unprecedented scale.

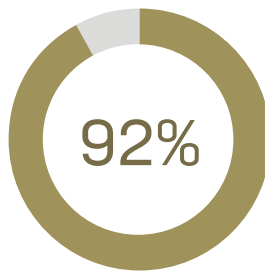
* Source: [Constella's 2024 Identity Breach Report](#)

Verizon 2024 DBIR Report Stats

1

RANSOMWARE AND EXTORTION THREATS

1/3 of all breaches in **2024** involved Ransomware or Extortion techniques, with **9%** of breaches being pure extortion attacks and **23%** involving ransomware. Combined, these stats show a growing trend in financially motivated attacks.



of industries saw prevalent ransomware and extortion threats, making them a top risk for executives and organizations alike.

2

THE HUMAN ELEMENT



68%

of breaches involved the human element, including social engineering, phishing, and credential theft.


25%

of financially motivated breaches were caused by Business Email Compromise (BEC) attacks, with a median transaction amount of \$50,000 per incident.

Cyber Threats Facing Executives in 2025 and Beyond

1. AI-Powered Social Engineering and Phishing

Cybercriminals have developed highly sophisticated social engineering and phishing techniques to target executives and HNW individuals. These scams exploit the vast amount of personal data available online to craft hyper-realistic emails, text messages, and even voice impersonations to deceive victims.

A man in a dark suit and glasses stands with his back to the camera, looking out a large window at a city skyline. The window is framed by dark vertical bars. The city is visible in the background, with several tall buildings. The scene is brightly lit, suggesting daytime.

One example is a deepfake heist in Hong Kong, where fraudsters used AI-generated voice cloning to impersonate a senior executive and authorize fraudulent transactions totaling **\$35 million.**

The ease of access to AI tools makes this a growing risk for high-profile individuals, whose online presence can be weaponized against them.

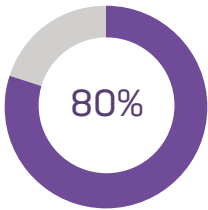
- AI-generated phishing campaigns now reduce attack costs by 95% while achieving equal or greater success rates than traditional phishing.
- Realistic deepfake impersonations enable hackers to mimic executives, manipulate employees, and authorize fraudulent transactions.
- Social media spoofing and impersonation attacks remain a top risk, allowing bad actors to hijack an executive's digital identity.

2. Data Breaches and Credential Exposure

When high-profile individuals are frequently featured in media and public databases, their personal and professional accounts become prime targets for exploitation.

A high-profile breach in 2023 involved LastPass, where attackers exfiltrated encrypted password vaults, putting thousands of executives and financial leaders at risk.

Once credentials are compromised, attackers sell them on dark web forums or use them to infiltrate sensitive corporate systems, leading to financial fraud, corporate espionage, or personal identity theft.



of individuals (including criminals) reuse passwords, increasing the likelihood of credential stuffing attacks.

The exposure of plaintext passwords doubled in 2023, with breached credentials appearing across dark web forums and data dumps.

2X
Plain text
passwords
exposure

Infostealers and botnets continue to be major threats, with cybercriminals leveraging malware to exfiltrate sensitive data from corporate devices.



3. Ransomware and Business Email Compromise

Ransomware and Business Email Compromise (BEC) attacks continue to be some of the most financially damaging threats to executives and wealthy individuals. Hackers are increasingly using pretexting tactics to manipulate executive assistants or finance teams into wiring funds..

In early 2025, the DOJ and Dutch National Police took down the Saim Raza/HeartSender cybercrime group responsible for a large-scale BEC network that resulted in more than \$3 million in losses and exposure of millions of data records.

Additionally, ransomware gangs such as RansomHub, Fog, and Lynx now target high-profile individuals and their families, demanding payments under the threat of releasing personal and financial data.

- The rise of Ransomware-as-a-Service (RaaS) has lowered the barrier for cybercriminals to deploy highly targeted attacks on executives.
- CEO fraud attacks cost companies between \$25,000 and \$75,000 on average, but some losses have reached tens of millions of dollars.
- The FBI's Internet Crime Complaint Center (IC3) reported over \$12.5 billion in losses in 2023, with BEC attacks being a major contributor.



Closing the Digital Protection Gap for Executives

To combat these evolving threats, organizations must adopt a proactive, multi-layered approach to digital executive protection. Real-time dark web monitoring, AI-driven threat intelligence, and executive identity risk management are critical components of a modern security strategy.

5 Best Practices for Digital Executive Protection

1 Mandate Real-Time Identity Monitoring

- Deploy automated tools that continuously scan the deep and dark web for exposed credentials, impersonation attempts, and leaked corporate data.
- Implement real-time breach alerts to notify security teams and executives of compromised information before it can be weaponized.

2 Enhance Authentication and Access Controls

- Enforce multi-factor authentication (MFA) across all executive accounts.
- Utilize biometric authentication and password managers to prevent credential reuse.
- Regularly rotate and update executive passwords to mitigate credential stuffing risks.

3 Protect Executive/HNWI Digital Footprint

- Regularly audit executives' online presence to remove outdated or risky information.
- Secure social media accounts with strong privacy settings and proactive brand protection services.
- Implement verified executive accounts to prevent impersonation.

4 AI-Powered Threat Intelligence Integration

- Leverage AI-driven security analytics to detect anomalies in email behavior and login attempts.
- Train employees on AI-generated phishing attack recognition.
- Automate security workflows to respond faster to emerging threats.

5 Adopt an Executive Protection Mindset

- Establish a dedicated executive cybersecurity task force to oversee digital risk management.
- Conduct quarterly cybersecurity training for executives and their assistants to stay ahead of new threats.
- Ensure executives' home networks and personal devices are secured with enterprise-grade security measures.



The Bottom Line

Cybercriminals continue to innovate, leveraging AI, dark web marketplaces, and automated malware to exploit executive vulnerabilities. Digital executive protection is no longer optional—it's a necessity. Organizations must prioritize proactive threat detection, robust authentication measures, and AI-driven security solutions to defend their leadership from evolving cyber threats. By implementing a multi-layered security approach, companies can significantly reduce risk and protect their executives—and their brand—from digital exploitation.



The FBI estimates that organizations victimized by CEO fraud attacks lose on average between \$25,000 and \$75,000. But some CEO fraud incidents over the past year have cost victim companies millions – if not tens of millions – of dollars.”



About Constella Intelligence

Constella.ai is the global leader in AI-driven identity risk and deep and dark web intelligence for such applications as identity theft, insider risk, Know Your Employee (KYE), Know Your Business (KYB), and deep OSINT investigations. With the world's largest breach database, containing over one trillion data attributes in 125+ countries and over 53 languages, Constella empowers leading organizations across the globe to monitor and secure critical data through unparalleled visibility and actionable insights. Ready for a secure future? Reach out to Constella today and stay one step ahead of digital threats.

Stay ahead of identity threats with AI-driven insights and unmatched intelligence.



www.constella.ai

contact email : constella@constellaintelligence.com