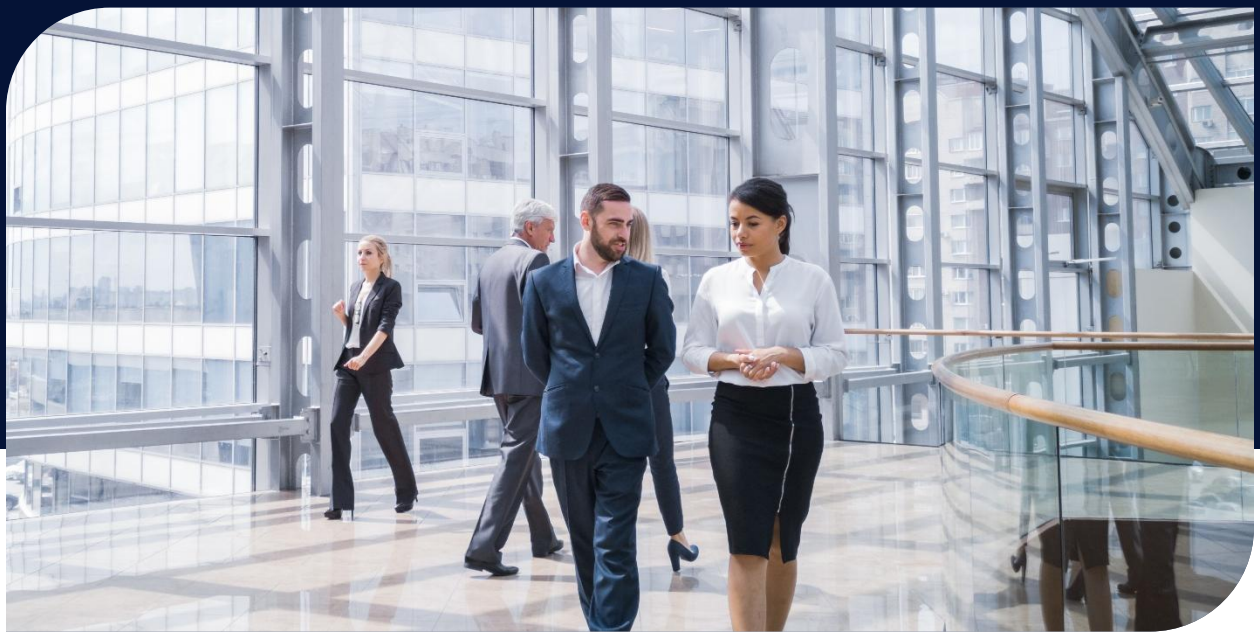
Teneo

Cyber Risk's New Frontier: The Leadership Attack Surface

Teneo Insights | March 2026



When adversaries can mimic leadership, the attack surface isn't just the network. It's also the people who run it. CEOs have learned to navigate volatility, regulation and geopolitical tension. Now, they face a new reality: adversaries breach systems by convincingly imitating leadership.

The role of the CEO has never been static. Over the past decade, chief executives have navigated expanding expectations, from geopolitical volatility and activist stakeholders to regulatory scrutiny, reputational risk and the accelerating pace of technological change. Each shift has redefined what leadership requires. Today's threat environment is no longer confined to networks or systems. It is shaped by adversaries who understand how organizations operate, how leaders communicate and how decisions are made under pressure, and then exploit that knowledge. Artificial intelligence has accelerated this transformation, enabling attackers to move beyond traditional intrusion toward influence, targeting the credibility and identity of senior leadership.

For CEOs and C-suite executives, cyber risk is no longer just something to oversee. It is something to personally navigate. The same visibility that defines modern leadership, including earnings calls, public interviews and digital presence, now provides adversaries with the raw material to replicate executive voices, mimic communication patterns and exploit organizational trust.

Recent reporting highlights the growing scope of this challenge, with AI-driven cyber fraud increasingly targeting executives directly and deepfake attempts rising across industries. These developments are not isolated technical trends. They represent a paradigm shift in the evolving threat landscape facing senior leaders that requires boards and executive teams to rethink how authority itself is protected. In this environment, protecting the enterprise increasingly means protecting the leadership layer.

The Rise of the Leadership Attack Surface

Traditional cyber models have always compromised infrastructure by gaining access through social engineering. AI now allows adversaries to mimic the highest levels of leadership behavior and exploit organizational trust to gain maximum access.

Business Email Compromise (BEC) campaigns, long one of the most profitable forms of cybercrime, now blends AI-generated emails, voice cloning, and synthetic video.[1] Generative AI enables attackers to craft communications that mirror internal tone and context, increasing credibility and accelerating action. Research shows that AI-generated spear phishing can perform as effectively as campaigns crafted by skilled human attackers, reflecting how automation has reshaped social engineering into a scalable enterprise.[2]

When the Attack Sounds Like You: How AI-Driven Cyber Campaigns Actually Work

The call comes from the CEO's number. The voice is familiar, calm, direct and slightly urgent. A confidential transaction needs approval and discretion matters more than process. Nothing about the interaction feels suspicious until it is too late.

Synthetic Executive Impersonation

Deepfake voice and video tools now allow attackers to convincingly mimic senior leaders using publicly available recordings. Fraud involving synthetic media has surged dramatically, with some analyses indicating growth exceeding 1,000 percent as AI tools become more accessible.[3] In one widely reported incident, attackers staged a video conference using AI-generated executives to persuade an employee to authorize a transfer exceeding $25 million, demonstrating how leadership identity itself has become a high-value attack vector.[4]

[1] Forty percent of business email compromise (BEC) are AI-generated

[2] Phishing Attack Statistics 2026 | Latest Trends, Facts & Data

[3] Deepfake Attacks & AI-Generated Phishing: 2025 Statistics

[4] Cybercrime: Lessons learned from a $25m deepfake attack | World Economic Forum

AI-Scaled Business Email Compromise

Models can generate highly personalized messages that reference internal projects, acquisitions or confidential initiatives. Reports indicate that roughly 40 percent of BEC messages may now involve AI-generated content, reflecting the rapid evolution of social engineering.[5,6] Before exploiting networks internally, attackers manipulate executive workflows turning organizational trust into an entry point.

Deepfake Voice and Real-Time "Vishing"

Voice phishing has evolved into interactive deception. AI-generated voices can respond dynamically during conversations, adjusting tone and urgency to maintain credibility. Surveys suggest many individuals struggle to distinguish AI-generated communications from authentic ones, highlighting the challenge facing organizations.[7] These attacks often exploit predictable executive behaviors: urgent requests tied to strategic deals, instructions to bypass controls or crisis scenarios designed to compress decision timelines.

This Changes the Boardroom Conversation

Deepfake detection remains difficult and executive preparedness varies widely across organizations[8], but one thing is clear: it requires a new model for reviewing cyber risk at the board level. Cyber maturity must extend beyond technology into leadership behavior, governance and crisis response frameworks. The leadership attack surface reframes cyber risk as a strategic issue requiring board oversight and integrated advisory support.

[5] Business Email Compromise Statistics 2026 (+Prevention Guide) - Hoxhunt

[6] Forty percent of business email compromise (BEC) are AI-generated

[7] Most adults couldn't differentiate between authentic, AI phishing emails

[8] Deepfake Attacks & AI-Generated Phishing: 2025 Statistics

Implications for Executives and Boards

If leadership itself becomes part of the attack surface, organizations must rethink resilience:

- **Authority alongside infrastructure.** Executive identity becomes a critical asset requiring protection in the same way today's cyber leaders protect systems and networks.
- **Decision velocity as risk exposure.** AI attacks compress timelines, forcing leaders to balance urgency with verification in a world of continually evolving technical advances.
- **Reputation as a part of the cyber domain.** Synthetic media can influence markets and stakeholders without breaching technical systems, requiring a layered strategic response that may initially seem technical but requires communications and a reputational risk management strategy.

Organizations that fail to adapt may find their next incident originates not from a network compromise but from a manipulated executive interaction.

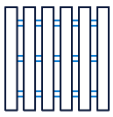
Teneo's Approach to Leadership Resilience

At Teneo, we ground our approach in practical reality and client autonomy. We work with leadership teams to clearly define their strategic priorities, map those priorities to evolving cyber and reputational risks and systematically address the vulnerabilities that emerge across their operating environment. Executive identity and visibility are treated as integral components of the attack surface, protected thoughtfully and proportionately based on each client's risk tolerance and desired level of resilience. Rather than imposing a one-size-fits-all solution, we build layered protections that align with how leaders operate, communicate and govern, ensuring security enhances decision-making rather than constraining it.

Cybersecurity Maturity Continuum

The Enterprise & Executive Perspective

Maturity Progression: From Minimal Security and High Exposure to Mature Cybersecurity Posture and Privacy by Design



High Risk Tolerance / Low-Cost Solutions

Minimal investment in security across the business. Reliance on basic tools (e.g., antivirus, firewalls). No formal protections for executive personnel.

- High likelihood of breach. Poor visibility, no formal incident response, minimal protection of customer and company data.
- Executives are prime targets with minimal safeguards. High risk of cyber security incident, email compromise, impersonation, doxxing and social engineering. Minimal protection of personal devices or home networks.

Moderate Security Investment

Core protections (e.g., MFA, endpoint security, basic user training) are implemented. Some executive protections may be considered (e.g., secure comms, separate accounts).

- Better defense against general threats. Foundational coverage for regulatory compliance. No advanced detection and response capabilities.
- Executives benefit from improved account controls (e.g., MFA, password managers) but are still vulnerable to tailored attacks. Public exposure and family risk unaddressed.

Aggressive Defensive Posture

Security is treated as a business-critical function. Advanced tools (e.g., threat intelligence, SIEM, DLP, EDR) are deployed. Executive protection is formalized.

- Comprehensive coverage across the enterprise. Faster detection and response and improved continuity, third-party oversight and compliance posture.
- Executives benefit from VIP threat monitoring, protected mobile devices, secure communications and personal cybersecurity hygiene support.

Extreme Privacy

Privacy and security are built into all systems and executive activities. Zero-trust model, privacy-by-design and encryption-by-default are implemented organization-wide.

- Strategic resilience. Data is segmented, encrypted and tightly governed. Compliance exceeds minimum requirements. IP is strongly protected.
- Executives benefit from pseudonymized travel, private threat monitoring, strong home network security and minimal digital footprint. Personal risk is proactively managed and mitigated.

We view executive and corporate cyber resilience along a continuum where the executive and the organization decide on the level of risk tolerance, investment and resilience commensurate with the threat landscape. While a high-risk tolerance and low-cost solutions are one strategy, increasingly CEOs and the companies they run are demanding more aggressive structures and, in some instances depending on the executive and the sector in which they operate, extreme privacy.

Cyber Risk in the Age of Synthetic Adversaries

Cyber risk has entered a new frontier defined not by systems alone but also by leadership itself. Artificial intelligence has advanced attackers, making them capable of mimicking authority, shaping decisions and influencing strategy alongside breaching infrastructure. Protecting infrastructure is no longer enough.

The next breach could begin with a perfectly convincing voice.

Authors

Courtney Adante
Global Head of Security Risk

Elizabeth Buckley
Managing Director, Head of
Cyber and Technical Solutions

Teneo
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance and ESG.

The firm has more than 1,800 employees located in 45+ offices around the world.

teneo.com