GetReal

Deepfakes:

A Material Risk to Leadership Trust

“Deepfakes turn executive identity into an attack surface — no breach required.”

What Board Directors and CEOs Need to Know Now

Advances in AI now make it possible to convincingly impersonate executives in voice and video interactions across the extended enterprise. This turns leadership identity, authority, and credibility into exploitable attack surfaces. Deepfake incidents no longer require system breaches or insider access. They exploit trust, urgency, and executive authority to trigger financial loss, reputational damage, and governance failures — often within minutes.

For boards and CEOs responsible for enterprise trust and operational integrity, this represents a new class of enterprise risk: one that bypasses traditional controls and directly impacts fiduciary oversight, market confidence, and organizational trust. Board members and executives represent a unique risk exposure because they combine high public visibility with authority that overrides controls and can trigger immediate action by employees and business partners. Attackers no longer need to compromise systems, only convincingly replicate a Board Director or CEO to commit fraud or damage company brands and executive reputations.

Why This Is a Board-Level Issue

Deepfakes risk intersects directly with areas under board responsibility:

- **Financial oversight:** fraudulent payments authorized via fake executive communications
- **Reputational risk:** false statements or announcements attributed to leadership
- **Market integrity:** misinformation that can move stock price or investor sentiment
- **Governance & duty of care:** growing expectations of preparedness for AI-driven threats
- **Organizational stability:** employee uncertainty during moments that demand clarity

What “Reasonable Preparedness” Looks Like

Leading organizations are beginning to implement controls aligned with how deepfake attacks actually occur:

- **Executive identity protection:** Monitoring and safeguarding voice, video, and likeness misuse
- **Authentication standards for high-risk actions:** Implement zero-trust principles in internal and external digital interactions
- **Employee awareness and training:** Teaching verification behaviors, not “spot-the-fake” guesswork
- **Crisis response playbooks:** Clear processes for rapid response to synthetic media incidents
- **Ongoing monitoring and takedown:** Detecting and responding to impersonation in the wild

Real Consequences

This is not a hypothetical risk. Incidents are already occurring across industries, and impact does not depend on size, sector, or technical maturity.

- In January 2026, a deepfake voice scam duped a Swiss businessman into transferring several million Swiss francs after attackers mimicked a trusted partner’s voice. (Source)
- In 2025, reporting shows deepfake scams cost victims over $200 million in just three months, with fraudsters using AI-generated audio and video to deceive adopters of remote communication tools. (Source)
- In 2024, a multinational firm’s finance director was fooled by a deepfake video call with synthetic executives and authorized a fraudulent fund transfer — a real example of video-based business fraud (reported in industry analysis). (Source)

Bottom Line

Deepfakes erode the foundation of corporate trust. Preparedness is now a leadership responsibility and a board-level oversight issue.

Recommendation

Treat deepfake risk as a standing agenda item alongside cyber, fraud, and reputation. Explore implementing solutions that prevent deepfakes in audiovisual environments and authentication solutions that are “deepfake resistant.”

About GetReal Security

GetReal Security is the cybersecurity leader specializing in the detection and mitigation of threats posed by malicious generative AI content including deepfakes and impersonation attacks. Its technology serves multinational corporations, financial institutions, media organizations, government agencies, and social media companies.

The company was incubated by Ballistic Ventures, the venture capital firm dedicated exclusively to funding and incubating entrepreneurs and innovations in cybersecurity, and Dr. Hany Farid, the preeminent expert in media forensics.

getrealsecurity.com