GetReal

Deepfakes:

Identity Threats Bypassing Legacy Security Stacks

> “Deepfakes are identity attacks operating outside of traditional detection and response.”

What CISOs Need to Know Now

Identity-based attacks are bypassing your infrastructure defenses. AI-generated voice and video are being weaponized to impersonate employees, executives, and trusted partners during live interactions — situations where technical controls can't intervene. These attacks don't exploit vulnerabilities in your systems. They exploit assumed identity in conversations, enabling unauthorized access and fraudulent approvals where your security stack lacks visibility.

No malware. No phishing links. No alerts.

Attackers now use deepfakes to manipulate help desk personnel, impersonate leadership on live calls, and bypass multi-factor authentication through social engineering at the audiovisual layer in your digital communications. When identity verification relies on voice recognition or video presence — and when authentication happens through human judgment rather than technical validation — your security perimeter moves outside the reach of your controls.

Why This Is a CISO-Level Issue

CISOs manage security risk, prevent unauthorized access, and limit blast radius, but deepfakes create exposure in a space traditional controls can't reach.

Deepfake-enabled attacks succeed by exploiting the gap between technical security and human workflows:

- **Controls bypassed through misplaced trust:** MFA and IAM verify credentials, not the person on a video call requesting credential resets or emergency access

- **Incident attribution and board exposure:** When a deepfake-enabled breach occurs, leadership and regulators look to the CISO for answers and ownership of the risk

- **Scope creep beyond your domain:** While CISOs don't own HR or finance workflows or IAM, you are, rightly or wrongly, perceived as responsible for the security failure when those processes are compromised

- **Regulatory and compliance implications:** Unauthorized access via impersonation triggers breach notification, forensic investigation, and regulatory scrutiny under your purview

- **Stakeholder confidence:** Board members are asking "what are we doing about deepfakes" — and expect CISOs to have answers

What "Reasonable Preparedness" Looks Like

Leading security organizations are implementing controls designed for the reality that seeing and hearing are no longer sufficient for identity verification:

- **Identity verification in human workflows:** Implement out-of-band verification for high-risk actions (credential resets, access requests, financial approvals) using separate, pre-established channels

- **Enhanced logging and attestation:** Require documented evidence of "who verified what, how, and when" for critical access decisions

- **Security awareness evolution:** Move beyond "spot the fake" training to verification behaviors and procedural discipline

- **Cross-functional security controls:** Close gaps between HR, IT, and Finance where deepfake attacks exploit disconnected verification processes

- **Real-time threat intelligence:** Understand the adversary behind an attack and indicators of compromise for deepfake-enabled campaigns targeting your industry or peer organizations

- **Incident response readiness:** Establish playbooks for suspected deepfake incidents, including immediate containment and forensic preservation

Real Consequences

This is not a theoretical risk. Security incidents involving deepfakes are already causing material losses and control failures:

- In 2024, a finance employee at multinational engineering firm Arup transferred $25 million after joining a video conference call with deepfaked executives, later confirmed to be entirely AI-generated. The attack bypassed all technical controls by exploiting trust in visual and audio authentication. (Source)
- Multiple Fortune 500 companies have reported account takeovers that began with help desk social engineering, where attackers used AI-generated voices to convincingly impersonate employees and request credential resets — no malware required. The FBI issued public warnings in 2024 that AI-crafted voice, video, and messages are actively being used for fraud and unauthorized access. (Source)
- Throughout 2024-2025, North Korean state-linked operators used fake identities and live video interactions enhanced by deepfakes to gain employment and access to corporate environments, bypassing traditional security screening. Federal authorities have documented hundreds of companies affected, with some cases resulting in data theft and extortion. (Source)
- Social engineering attacks using deepfakes became the leading initial access vector in incident response cases from mid-2024 to mid-2025, accounting for 36% of all incidents, with two-thirds targeting privileged or executive accounts specifically. (Source)

Bottom Line

Deepfakes are identity threats that exist outside the traditional security perimeter and require detection and response capabilities. Preparedness requires extending controls into human interactions and business workflows where identity verification doesn’t currently exist.

Recommendation

Treat deepfake-enabled identity attacks as a standing security risk requiring cross-functional controls, enhanced verification processes, and continuous adaptation as attack sophistication increases. Invest in solutions that provide verification beyond what users see and hear.

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