GetReal

Deepfakes:

The Trust Layer Built for Remote Work Is Being Exploited

“Deepfakes make the trust layer that enables remote work and collaboration an attack surface.”

What CIOs Need to Know Now

The digital transformation and remote collaboration infrastructure you built to enable business agility has created a new attack surface: synthetic identity in live interactions. AI-generated voice and video are being used to impersonate employees, executives, and trusted partners across the collaboration platforms, help desk workflows, and remote access systems that IT delivers and supports.

These attacks don't target your infrastructure. They exploit the trust assumptions embedded in how your organization uses that infrastructure — specifically, the belief that video calls, voice authentication, and real-time communication verify who people claim to be. When attackers can convincingly replicate identity during live interactions, they bypass technical controls and manipulate human workflows to gain access, authorize changes, and disrupt operations.

This creates direct exposure for CIOs. You own service delivery, operational stability, and technology enablement. When deepfakes compromise help desk processes, remote access workflows, or executive communications, the resulting business disruption, security incidents, and remediation costs fall under IT operations.

Why This Is a CIO-Level Issue

While you deliver secure, reliable IT services that enable business operations, deepfake attacks exploit the seams between technology and human judgment, creating risk across multiple dimensions:

- **Help desk and IT support compromise:** Attackers use deepfake audio to impersonate employees requesting password resets, MFA re-provisioning, or access to systems — successfully manipulating IT support staff who rely on voice recognition and verification questions
- **Business continuity and operational disruption:** Deepfake-enabled incidents can halt operations, trigger emergency response, and consume IT resources in forensic investigation and remediation
- **Technology enablement risk:** Remote work tools, video conferencing platforms, and collaboration software become vectors for impersonation attacks, raising questions about whether IT-provided capabilities create unmanaged risk
- **Digital transformation delays:** Security incidents involving deepfakes can slow or halt AI adoption, cloud migration, and digital initiatives as leadership demands assurance that new capabilities won't introduce similar vulnerabilities
- **Stakeholder accountability:** When deepfake attacks succeed, CIOs must explain to the board and executive leadership why IT-supported workflows allowed unauthorized access or fraudulent authorization
- **Cross-functional tension:** Deepfake incidents expose gaps between IT, Security, HR, and Finance — and CIOs can be looked to for coordinating the response even when root causes lie outside IT's direct control

What "Reasonable Preparedness" Looks Like

Leading IT organizations are implementing controls and processes designed to address the reality that collaboration platforms and remote access tools can be exploited through identity impersonation:

- **Enhanced verification for IT support workflows:** Implement out-of-band verification for high-risk IT requests (password resets, MFA changes, access provisioning) using pre-established channels — designed to add security without creating friction for legitimate users
- **Deepfake detection and help desk training:** Deploy real-time detection tools that identify synthetic voice and video during live interactions, and train IT support teams to recognize deepfake indicators and follow verification protocols even under pressure
- **Identity verification in ITSM workflows:** Embed stronger identity verification into IT service management, particularly for privileged access and security-sensitive changes, while maintaining streamlined experiences for verified users
- **Incident response and coordination:** Establish clear playbooks for responding to suspected deepfake incidents, with defined roles across IT, Security, HR, and business units
- **Continuous threat intelligence:** Monitor deepfake attack techniques targeting IT operations and adjust controls as threat sophistication evolves

Real Consequences

Deepfake attacks targeting IT operations and collaboration infrastructure are already causing material incidents across industries:

- **Social engineering became the leading initial access vector** (36% of incidents from mid-2024 to mid-2025), with two-thirds targeting privileged or executive accounts through help desk manipulation. (Source)
- **Voice phishing surged 442%** in 2024, driven by AI voice cloning allowing attackers to impersonate employees during IT support calls. Threat actors increasingly abandoned malware in favor of targeting help desks directly. (Source)
- **$25 million transferred at Arup** after a finance employee joined a video call with deepfaked executives on a collaboration platform — exploiting trust in remote work infrastructure. (Source)
- **North Korean operatives increasingly use deepfakes** to pass video interviews and gain employment as IT workers at hundreds of U.S. companies, then used access to steal data and conduct extortion. (Source)

Bottom Line

Deepfakes turn remote collaboration and IT support workflows into attack vectors. Zero trust secures infrastructure access, but doesn’t extend into the live audio, video, and human interaction layer where employees can be deceived. CIOs must address this gap or accept operational risk.

Recommendation

Treat deepfake risk as a technology enablement and operational resilience issue, not just a security problem. Implement verification controls in IT support workflows, harden collaboration platforms against impersonation, and establish clear protocols for responding to suspected deepfake incidents. Consider deepfake preparedness a prerequisite for sustaining digital transformation and AI adoption initiatives.

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