Deepfake & Executive Impersonation Defence

Cyberfort
Expert-led. Security Driven.

Protect executives and finance teams from AI-powered impersonation fraud

Introduction

Artificial intelligence has handed attackers a capability that no firewall, endpoint agent, or email filter was designed to stop: the ability to convincingly impersonate your CEO, CFO, or board members in real time, at scale, and at a minimal cost.

Deepfake audio, synthetic video, and AI-generated written impersonation are no longer theoretical risks confined to nation-state actors. They are live, commercially available, and being deployed against organisations of every size and sector right now.

Cyberfort's Deepfake & Executive Impersonation Defence service is built for the reality that your most dangerous attack surface is no longer your technology; it is the human trust your organisation runs on.

What is the Deepfake & Executive Impersonation Situation organisations are facing?

Your organisation almost certainly has executives whose voices, faces, and communication styles are publicly accessible - on LinkedIn, YouTube, investor calls, press interviews, and company websites. That public presence, once an asset, is now raw material for adversaries.

Finance teams authorise payments on the instruction of senior leaders. HR teams process sensitive requests based on executive direction. Board members make decisions informed by briefings they trust are genuine. In each case, the verification mechanism is human judgement, and human judgement is precisely what AI-powered impersonation is engineered to defeat.

If your organisation handles significant financial transactions, holds sensitive data, operates in regulated industries, or has executives with any public profile, you are already a target. The question is not whether an attempt will be made, it is whether your people will recognise it when it happens.

Key challenges with this type of attack

Traditional security controls are blind to this threat. Deepfake attacks don't arrive as malware. They don't trigger DLP rules or SIEM alerts. These types of attack exploit communication channels, a phone call, a video message, a WhatsApp voice note, that your security stack was never designed to monitor.

Awareness alone is not enough. Generic phishing training does not prepare employees to question a call from someone who sounds exactly like their CEO, or a video message that looks indistinguishable from a real briefing. Without specific, scenario-based preparation, even security-conscious staff can be deceived.

The attack surface is growing faster than defences. The tools required to clone a voice or generate a convincing synthetic video are now freely available and require no technical expertise. The barrier to entry for attackers has collapsed.

Meanwhile, most organisations have no formal process for verifying executive identity in high-risk scenarios. Exposure is often invisible until it's too late. Most organisations have no clear picture of how much publicly available material exists that could be used to train an impersonation model against their executives, and no process for assessing or reducing that exposure.

The impact of Deepfake Attacks

41%

of organisations have experienced a deepfake combined with a social engineering attack on an audio call

Gartner 2026 CISO Role-Based Survey

1500%

increase in Deepfake attacks since 2023

UK Gov - Innovating to detect deepfakes and protect the public

Over **£210,000**

what a successful Deepfake attack costs a business on average

Ironscales 2025 Beyond Detection Reality of Deepfakes Report

These numbers tell a consistent story: the rise of publicly available generative AI means attacks that previously required sophisticated criminal groups can now be launched by individuals with little technical expertise. The volume is exploding, the average loss is material, and nearly half of organisations have already been targeted. Organisations that have not yet experienced an attempt are not protected - they might be next.

When Does This Service Become Particularly Relevant?

You should be talking to us if any of the following apply:

- Your CEO, CFO, or other senior executives are active on LinkedIn, appear in press coverage, or feature in publicly available video or audio content
- You are a publicly listed company or have executives in frequently quoted, high-profile roles
- You have recently experienced a fraud attempt involving impersonation or social engineering
- Your finance team operates large payment approval processes, particularly those involving same-day or urgent transfers
- Your organisation is going through a merger, acquisition, or significant restructuring, when financial instructions increase in volume and urgency
- Your sector is subject to regulatory scrutiny around financial controls, data protection, or operational resilience

If you recognise your organisation in any of these scenarios, your exposure is real and the window to act before an incident is now.

Who is this service for?

This service is designed for organisations where the cost of a deepfake attack is likely to impact revenue, customer relationships or industry reputation.

- CFO's or Finance Directors responsible for payment authorisation and financial controls
- CIO's and Risk Directors managing emerging AI threat exposure
- CEO's and board members with a significant public profile
- HR Directors overseeing sensitive executive-instruction processes

What does a typical engagement for this service look like?

This is not a six-month consulting engagement. It is a focused, expert-led programme designed to get you from exposed to protected in a short period of time.

1

Step 1 - Exposure Mapping

Our consultants conduct the Executive Exposure Review, systematically mapping all publicly available material video, audio, written content, social media, that could be used to train an impersonation model against your key individuals. You receive a prioritised exposure report.

2

Step 2 - Risk Assessment and Scenario Design

We complete the Deepfake Risk Assessment, identifying your highest-risk roles, communication channels, and financial processes. We design bespoke fraud scenarios based on your actual organisation structure and payment workflows.

3

Step 3 - Fraud Scenario Testing and Training

Your finance, HR, and executive teams go through realistic AI impersonation simulations. We debrief, identify where human controls held and where they didn't, and deliver targeted AI Awareness Training tailored to your scenarios.

4

Step 4 - Playbook Delivery

We hand over the Executive Protection Playbook - verification protocols, out-of-band confirmation procedures, escalation paths, and governance processes your organisation can embed immediately and sustain independently.

The result

Board-level assurance that this emerging threat class is being actively managed, delivered in a timeframe that matches the urgency of the risk.

Key Deliverables

- Executive Exposure Review
- Deepfake Risk Assessment
- Fraud Scenario Testing
- AI Awareness Training
- Executive Protection Playbook

Business Value of this service

- Reduce exposure to deepfake-enabled fraud and payment scams
- Protect executives, finance teams and HR leadership
- Improve resilience against AI-enabled social engineering
- Provide board-level assurance around emerging AI threats

Key Outcomes from this service

Organisations that complete Cyberfort's Deepfake & Executive Impersonation Defence engagement leave with:

An Executive Exposure Review that maps publicly available material that could be used to impersonate key individuals, so you can take informed action to reduce it.

A structured Deepfake Risk Assessment that identifies your highest-risk scenarios, roles, and communication channels, giving you a prioritised view of where to focus.

Tested resilience through Fraud Scenario Testing that puts your finance, HR, and executive teams through realistic AI impersonation simulations, so you know exactly where your human controls hold and where they don't, before an attacker finds out for you.

Trained and prepared people - Targeted AI Awareness Training that moves beyond generic phishing content to give your teams the specific knowledge and verification instincts they need to identify and challenge AI-generated impersonation attempts.

An Executive Protection Playbook that embeds durable, practical controls: verification protocols, out-of-band confirmation procedures, escalation paths, and governance processes that keep pace with a fast-evolving threat.

The result is an organisation that has moved from unknowing exposure to active, measurable resilience, with board-level assurance that this emerging threat class is being managed.

What our customers say about this service

"We thought our controls were solid until Cyberfort ran the scenario testing. Watching a member of our finance team nearly authorise a six-figure transfer based on a synthetic audio call from someone who sounded exactly like our CFO was a wake-up call we needed to have in a controlled environment rather than a real one."

Head of Information Security, UK Financial Services Firm

Next Steps

Book a 30-minute call with one of our executive impersonation defence specialists to understand your current exposure and what an attacker could do with what's already publicly available about your leadership team.

Contact us at info@cyberfortgroup.com or call +44 (0)1304 814800 to arrange your call.

To find out more about our full range of cyber security services, visit cyberfortgroup.com

Cyberfort
Expert-led. Security Driven.

DATA SHEET