KPMG

Europe at a crossroads

Deepfakes: what every CEO should know about the new face of deception

Edward Amoroso

February 2026

Deepfakes: what every CEO should know about the new face of deception

What if your next PR crisis doesn't come from something one of your leaders said, but from what someone made it look like they said? It could destroy the reputation of your organisation. Therefore, deepfakes deserve to be on the agenda of any CEO. C-suite should treat deepfakes not as a technological anomaly, but as a permanent feature of the business landscape.

Not so long ago, deepfakes were internet curiosities. Think of synthetic videos of politicians saying absurd things or the pope dressed in extravagant clothes. Maybe fun to watch, not much to worry about. Today, every CEO should be treating **deepfakes as a whole new corporate risk category**. As generative AI accelerates, so does the ability to convincingly fake voices, faces, and entire video calls.

What once required a Hollywood studio can now be done on a laptop. In 2024, several companies, such as the famous case of Arup, a global design firm, reported scams where fraudsters cloned executives' voices to authorise wire transfers. It is important to note that the threat goes far beyond financial fraud. Imagine a deepfake of a CEO announcing layoffs, or a fake video showing a product defect.

In an age where reputations can collapse in hours, a single viral clip can move markets. Researchers have warned that deepfake audio could be used to fabricate earnings call transcripts or investor briefings. A convincing fake could manipulate stock prices or trigger regulatory scrutiny before the truth is uncovered. Unlike traditional phishing or malware, deepfakes target perception. They blur the line between truth and fabrication, making it difficult to trust what we see.

There is no doubt: the risks are real. **But smart executives know how to flip risk into opportunity.** They are aware that defending trust may give them a competitive advantage. So, the question is: how can C-level do this effectively?

Below you'll find a breakdown of some takeaways and practical strategies for executive teams, based on our own expertise and the insights of Edward Amoroso, cybersecurity veteran and founder of TAG Cyber.

Use detection technologies

The first line of defence is technological. There are many promising innovations from universities and startups that analyse images and videos to assess their authenticity. These range from startups like Originality.ai, promising 99% accuracy, to OpenAI that develops its own detection tools. These pioneering tools can detect synthetic media by examining metadata, pixel inconsistencies, and source anomalies. Insurance companies use them in their claim processes.

For executives, this means investing in or partnering with vendors who specialise in deepfake detection. These tools can be integrated into social media monitoring, PR workflows, and incident response plans. While the technology is still evolving, early adoption positions your organisation ahead of the curve. Having said that, mala fide attackers tend to quickly adapt to defence strategies and the **classic arms race in cyber is also taking place in this relatively new risk category.**

Actionable advice

- Ask your CISO or CTO to evaluate deepfake detection vendors.
- Pilot tools that assess media authenticity in high-risk channels (e.g., executive communications, investor relations).
- Stay informed about academic research and emerging standards in synthetic media analysis.

Define a rapid response policy

Reputation is fragile. A single deepfake video of a CEO can trigger stock volatility, customer backlash, or regulatory scrutiny. This isn't just about technology. It's also about readiness. Having a trusted partner who can validate or debunk suspicious content within hours is critical. It's akin to having a crisis PR firm on retainer, but for digital authenticity.

Actionable advice

- Identify and onboard a deepfake response vendor as part of your incident response plan.
- Conduct tabletop exercises simulating a deepfake attack on your leadership team.
- Ensure your legal and communications teams are trained to handle synthetic media crises.

Advocate for provenance and transparency

Imagine hovering over a photo or video feed and instantly seeing its creation date, device ID, and digital signature. This level of transparency could transform how media is trusted and shared. While the infrastructure to get to this scenario isn't fully in place, C-level leaders can champion this shift by demanding provenance from vendors and platforms. Several initiatives such as the Content Authenticity Initiative (CAI) aim to implement this on a large scale.

Edward speaks of **the concept of a 'bill of materials' for media** in this respect. This would involve embedding metadata into images and videos that verify their origin, using cryptographic signatures or blockchain.

Actionable advice

- Encourage your marketing and content teams to embed origin metadata in all official media.
- Support industry initiatives that promote media provenance standards.
- Explore blockchain-based solutions for media verification in high-stakes environments.

A cultural shift toward scepticism

"In the past it often made sense to believe something until it was debunked, in the future it will start to make sense to assume they are fake unless they are verified." Technology magazine Wired wrote this in 2019 and it is safe to say that this future has now arrived.

This is a cultural shift. Just as employees have learned to question suspicious emails, they must now learn to question visual content. **Instinctive scepticism will become a vital skill.**

Executives should lead by example, promoting media literacy and critical thinking across the organisation. This isn't about paranoia, it's about resilience.

Actionable advice

- Launch internal awareness campaigns about deepfakes and synthetic media.
- Include media verification in cybersecurity training programs.
- Foster a culture where 'verify before you share' becomes second nature.

A final word

Deepfakes are unsettling, but they're not insurmountable. Cybersecurity has faced similar challenges before and has overcome them. With the right mix of technology, partnerships, and cultural adaptation, the C-suite can turn deepfake anxiety into strategic advantage.

Because in the age of synthetic media, **trust isn't just earned, it's engineered.**

Viewpoint
Bert Koelewijn

Deepfakes in the boardroom: what every CEO needs to put in place now

What if your next crisis is not caused by something you actually said, but by what the internet makes it look like you said? This is not a classic malware issue. It is a topic that attacks perception and trust. For the C-suite, the question is therefore not whether this risk will materialise, but how trust is structurally governed. A complex challenge, where the board can at least focus on the following priorities.

1. Anchor the risk in governance

Explicitly include synthetic media in the risk register (owned by the CISO, with Legal and Communications). Define clear thresholds: when does an incident qualify as a reputational crisis, market-sensitive information, or a privacy breach?

2. Invest selectively in detection without being naive

Integrate media authentication into social listening and PR workflows. Use detection tools as early-warning signals, not as sources of absolute truth. Always combine tooling with human judgment.

3. A 72-hour rapid response playbook

Define a clear triage route (who assesses, who verifies, who decides), prepare a holding statement, and pre-authorise takedown paths with platforms and registrars. Rehearse this scenario twice a year with the CEO and IR/PR.

4. Provenance and transparency of owned media

Publish CEO communications through verified channels with provenance or watermarking. Provide clear disclosure when using synthetic voice or media. Ensure content signing is embedded in the CMS.

5. Normalise scepticism, without paranoia

Make 'verify before you share' a standard reflex, from boardroom to service desk. Provide targeted awareness for high-risk roles (C-suite, Finance, IR), including practical audio and video spoofing exercises.