Faked to Perfection

The rise of deepfake threats against corporate executives

BLACKCLOAK®

Ponemon INSTITUTE

Publication Date: April 2025

About This Report

This report is an excerpt from "Deepfake Deception: How AI Harms the Fortunes and Reputation of Executives and Corporations," sponsored by BlackCloak and independently conducted by the Ponemon Institute, LLC.

Introduction

A deepfake is an artificial image or video generated by a form of artificial intelligence (AI) called deep learning. Typically, the attacker starts by collecting authentic media samples of their target to use as training material for the deep learning model. These samples include still images, videos and audio clips. The more training data the attacker acquires, the more authentic the resulting deepfake will appear.

To understand how prepared organizations are to address deepfake risks, BlackCloak commissioned the Ponemon Institute to survey US IT and security practitioners with working knowledge of deepfake risks and the impact to their organizations. The research uncovers important information about how organizations view the deepfake risk against board members and executives, and what steps are being taken to reduce these threats.

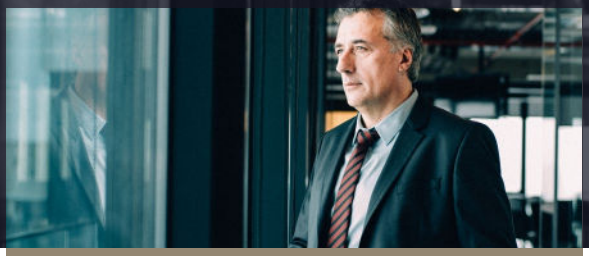
The results highlight that:

01. Deepfake risks are increasingly targeting vulnerable board members and executives

02. Organizations are suffering from a lack of visibility and preparedness to combat deepfake attacks

03. The consequences from deepfakes and cybersecurity threats are a serious concern

04. Deepfake is one of the most worrying uses of AI



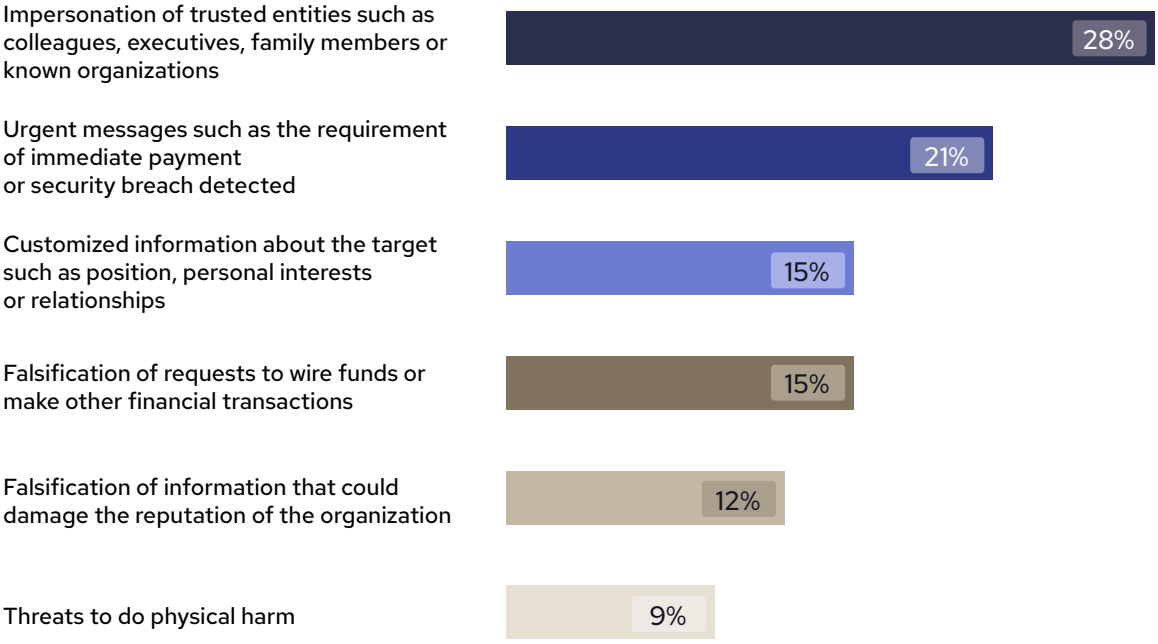
Deepfake risks are a growing concern

The survey reports that 42% of executives and board members have been targeted at least once by a fake image or video, over half of whom were targeted more than once. Despite growing awareness of the need for Digital Executive Protection, 18% of respondents were unsure whether their senior leadership team had been the target of a deepfake. The most common deepfakes experienced are impersonation of executives' trusted entities and urgent demands for payments or information about a detected security breach.

FIGURE 1

How deepfakes have targeted executives

One choice permitted. Total = 100%



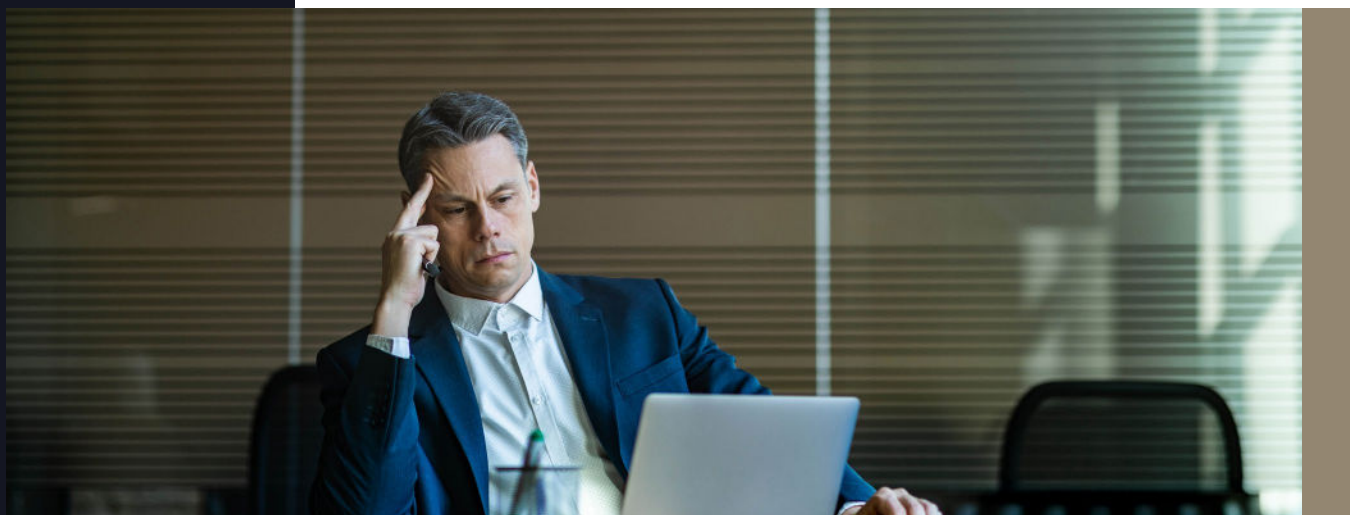
The future risk of deepfake threats

Looking ahead, IT and security professionals are anticipating continued growth of deepfake attacks, with 66% of respondents stating it is highly likely their executives will be targeted by a deepfake in the future, and 54% citing deepfake as one of the most worrying uses of artificial intelligence (AI).

FIGURE 2

Rate the likelihood of a future deepfake targeting your executives

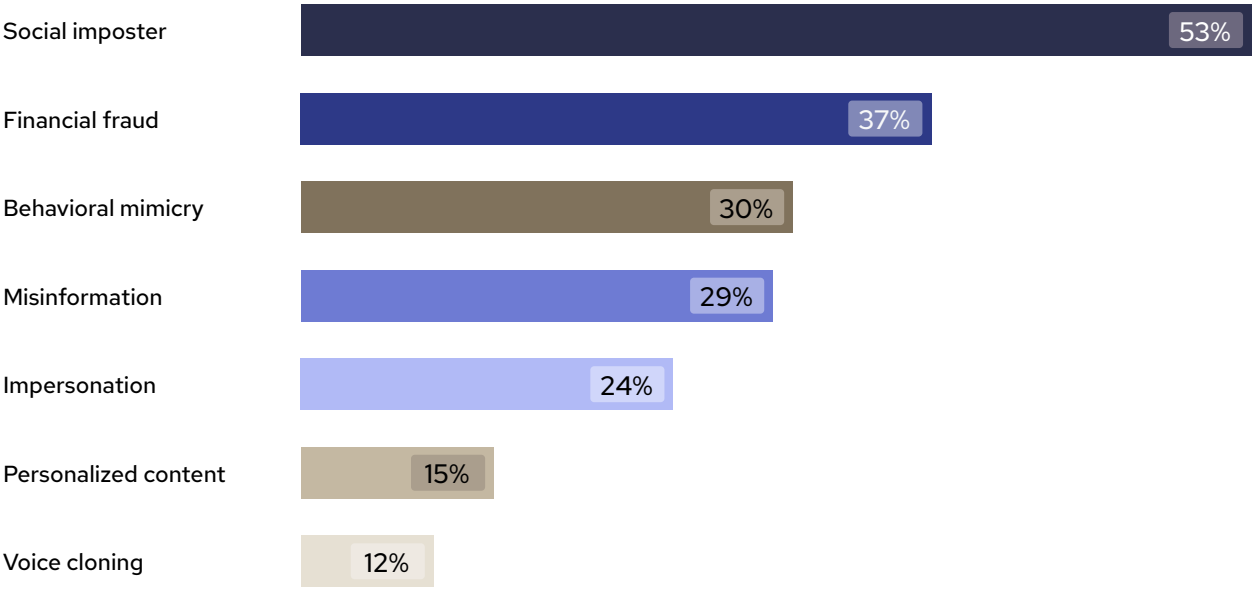
1 = not likely to 10 = highly likely. Total = 100%



The greatest concern is that of attacks from social imposters (53% of respondents) and financial fraudsters (37% of respondents).

FIGURE 3

What are the top two deepfake risks concerning your organization?



How prepared are organizations for a deepfake attack?

Fifty-nine percent of respondents say it is very or highly difficult to detect deepfake attacks. This could largely be due to lack of insight into malicious activity to prevent a deepfake threat, as 50% of respondents cited low-to-no visibility. Only 21% of respondents say their organizations have high visibility into the erroneous activity happening within their organization to prevent deepfake threats.

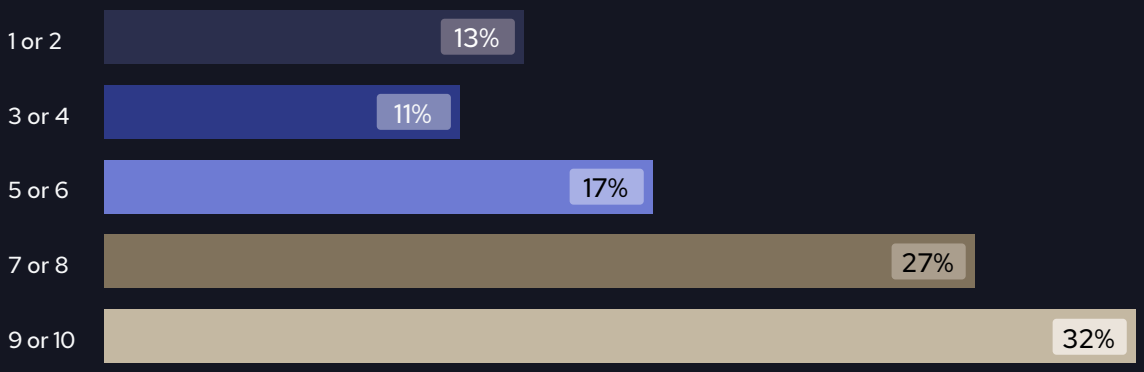
59%

respondents say their teams have little visibility to prevent deepfake threats

FIGURE 4

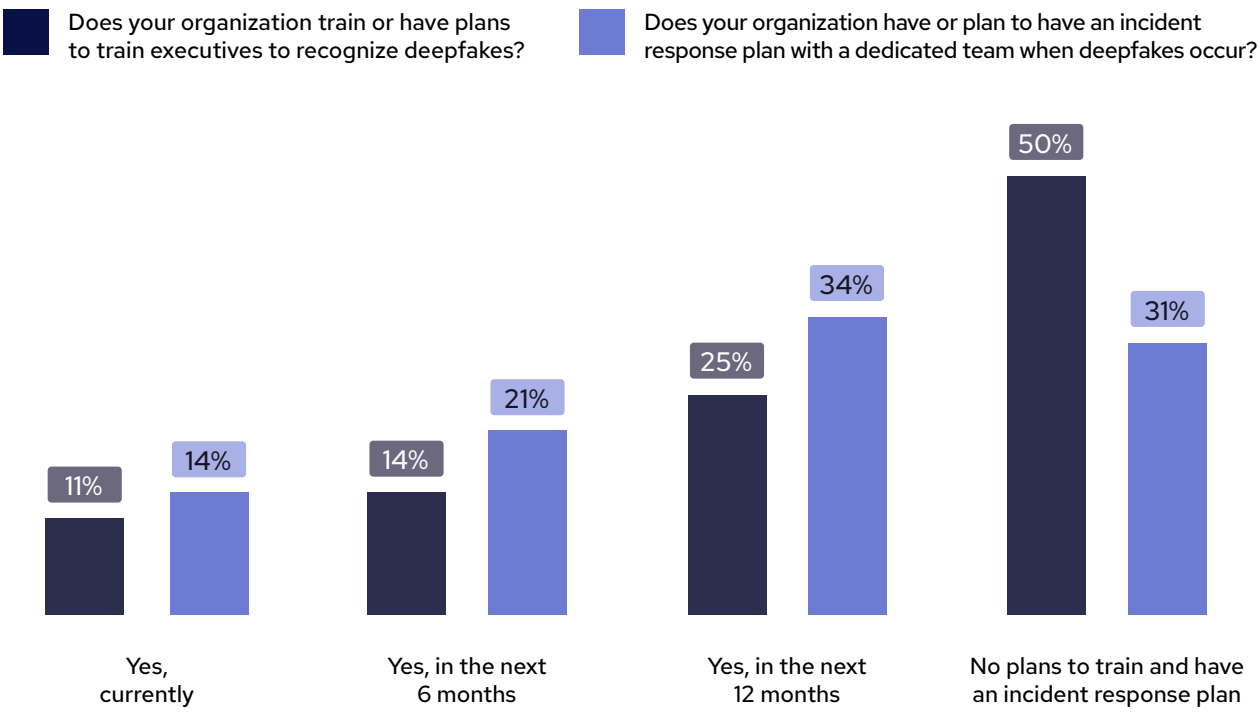
Rate the difficulty to detect a deepfake targeting your executives

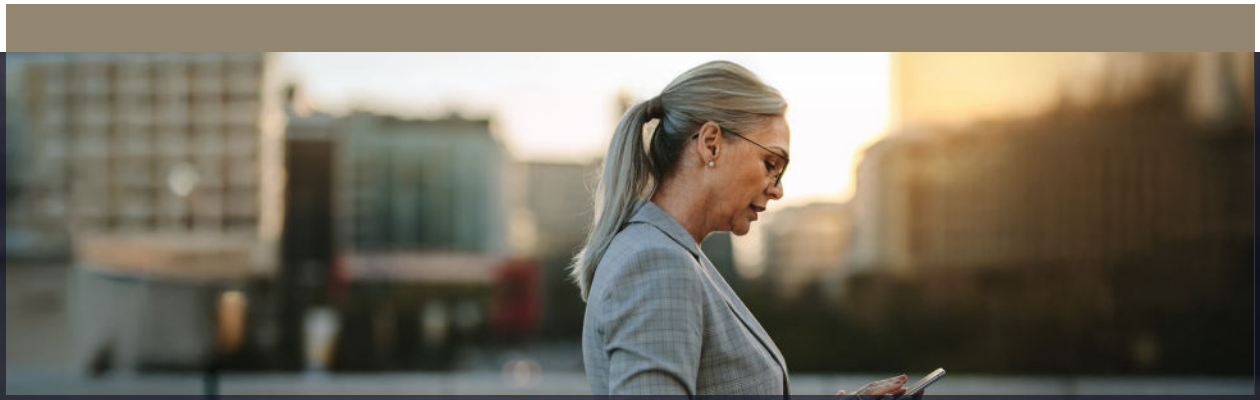
1 = not likely to 10 = highly likely. Total = 100%



Compounding the issue is the lack of confidence IT and security teams have in the ability of their executive team to recognize a deepfake risk when it occurs. However, despite these weaknesses in reducing the risk of an attack, 50% of respondents say their organizations do not plan to train executives on how to recognize an attack. Only 11% of respondents currently train executives to recognize deepfakes, and only 14% have an incident response plan with a dedicated team prepared for when deepfakes occur.

FIGURE 5





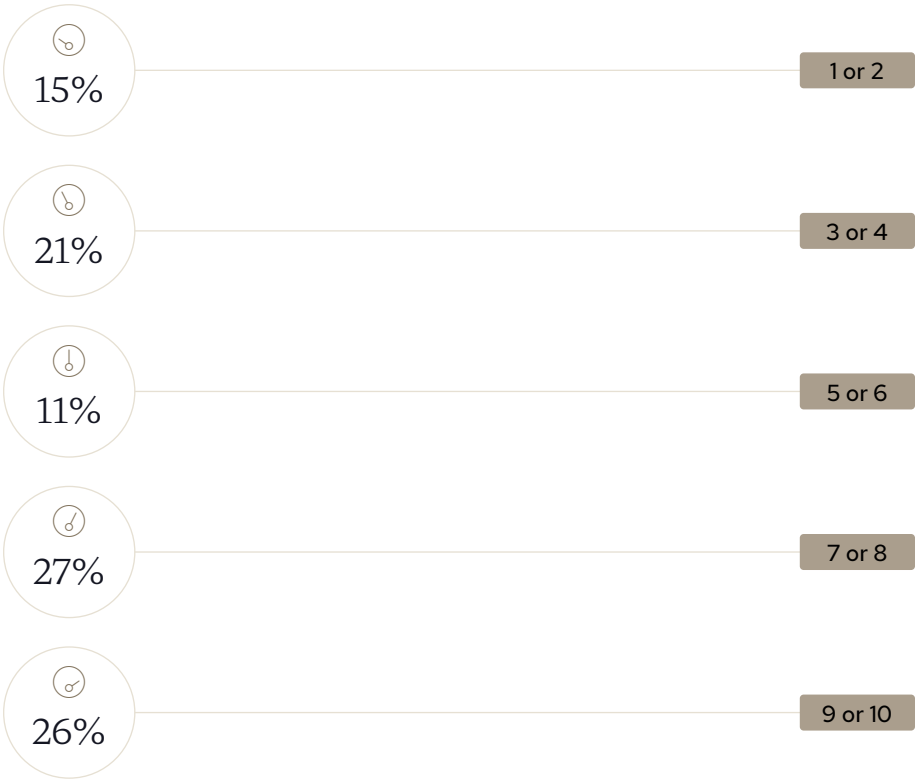
The importance of technology to reduce deepfake risks

The response to deepfake threats is not entirely apathetic; 56% of respondents agree executives must understand that a zero-trust mindset is essential to not becoming a deepfake victim. To support these efforts, it appears that investment in technology is the solution of choice. Fifty-two percent of respondents say it is highly likely that their organization will evaluate technologies that can reduce the risks from deepfakes targeting executives, and 53% of respondents say technologies that enable executives to verify the identity and authentication of messages they receive are highly important.

FIGURE 6

How important is technology to reduce the risk of a deepfake threat?

1 = not important to 10 = highly important. Total = 100%



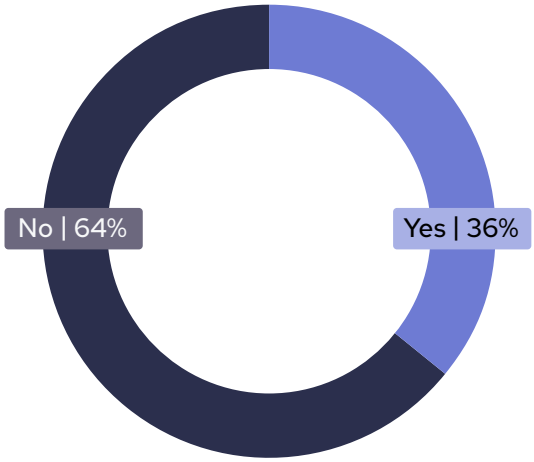
Measuring the impact of deepfake attacks

The financial consequences of deepfake attacks are not often measured and therefore not widely known. Only 36% of respondents say their organizations measure how much a deepfake attack can cost. Those who do cite the cost to detect, identify and remediate the breach (50% of respondents) and the cost of staff time to respond to the attack (46% of respondents) as the top metrics measured.

FIGURE 7

Have you measured the financial consequences of a deepfake targeting your executives?

Total = 100%



Summary

Deepfakes are reliant on copying a personal image, voice, tone and style of communication. The more personal data that exists across the clear, deep and dark web, the easier it is for AI to create realistic videos, social engineering campaigns and impersonate contacts to target executives.

Deepfakes are currently able to exploit organizations' limited preparedness and ability to detect them. As this threat becomes more prevalent, impersonating trusted entities and prompting fraudulent actions, organizations must increase their visibility, training, and response capabilities. Adopting a zero-trust approach, reducing the digital footprint of executives and investing in technology solutions to verify authenticity are critical steps toward effectively combating these increasingly common and damaging threats.

BLACKCLOAK®

BlackCloak protects corporate executives and high-profile individuals from cybersecurity, privacy, financial, and other reputational risks. Used by Fortune 500 companies across all industries, the BlackCloak Concierge Cybersecurity & Privacy™ Platform is a holistic solution that includes mobile and desktop apps and concierge support. Executives and high-profile individuals gain complete peace of mind knowing their family, reputation, and finances are secured. Companies rest assured that their brand, intellectual property, data, and finances are protected against threats from executives without invading their personal lives.

Learn more at www.blackcloak.io, and follow us on LinkedIn.

@BlackCloakCyber

BlackCloak

info@blackcloak.io

www.blackcloak.io