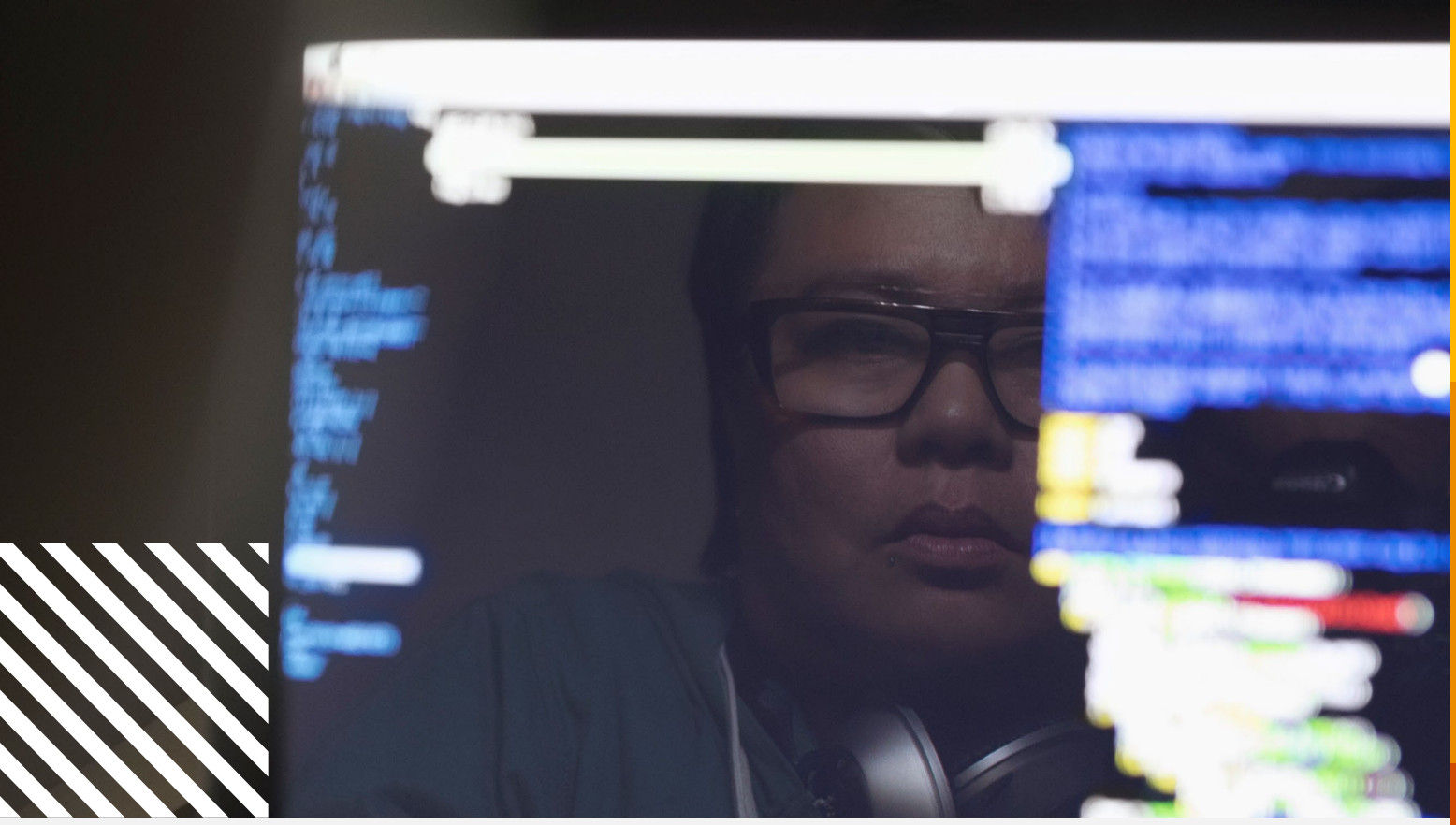


# The new face of fraud:

## Combating impersonation and deepfake threat

pwc

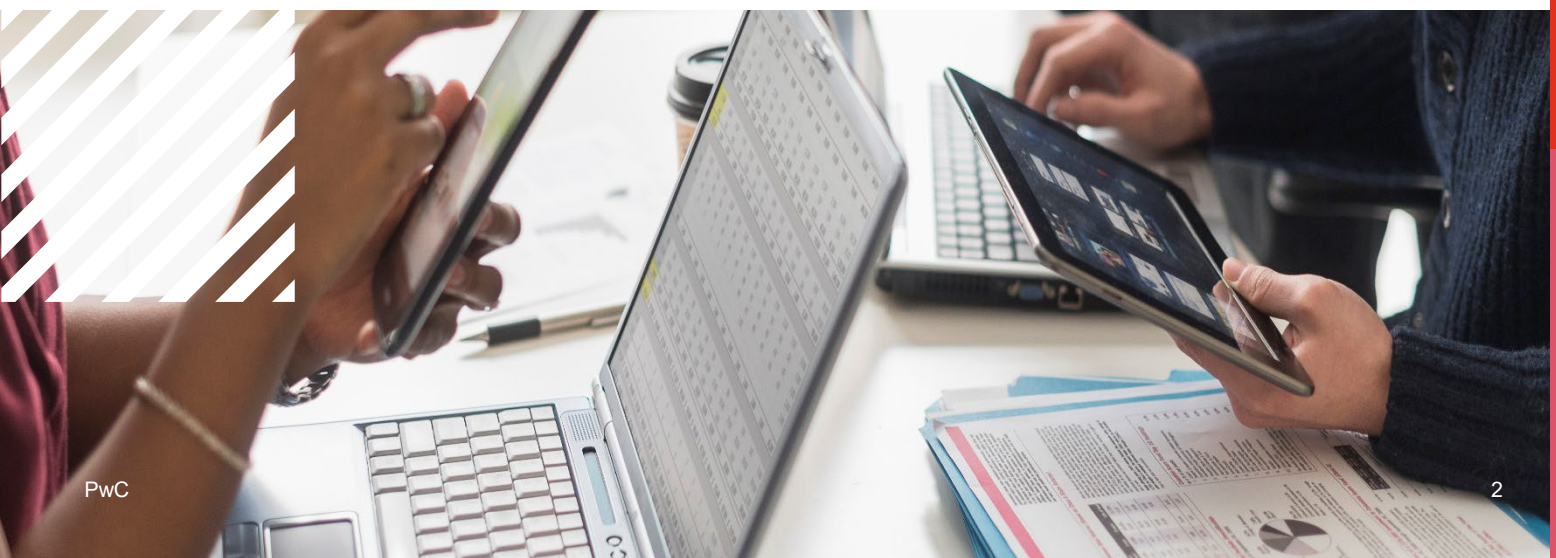
Imagine **a significant amount of money** was transferred from your company **bank account** authorised by a senior executive in your organisation.

**Later, however, you discover you have been a victim of fraud…**

Unfortunately, this scenario is becoming more and more common. At PwC, we are seeing this as a **growing global trend**—and Southeast Asia is no exception, with companies across several industry sectors **falling victim.**

According to the Global Economic Crime Survey 2024, cybercrime, including impersonation fraud using deepfake technology, is the top reported type of fraud across the world.

According to the Global Digital Trust Insights Report 2025, security executives report that GenAI (67%) and cloud technologies (66%) have expanded the cyberattack surface over the past year. This means companies are more vulnerable to sophisticated threats.



## What is impersonation fraud?

**Impersonation fraud is a growing threat** in our digital world where **criminals imitate legitimate representatives** of companies to steal sensitive information or money.

## This can include:

01

**Phishing:**

Fraudsters send deceptive emails pretending to be trustworthy individuals or organisations to trick people into providing sensitive information.

02

**Business email compromise:**

Cyber criminals use email-based social engineering to defraud businesses by impersonating executives or employees.

03

**Deepfakes:**

This involves the use of deepfake technology to mimic the voices or appearances of executives, often targeting junior staff or those less familiar with these individuals.

These techniques have become more sophisticated with AI and deepfake technology, making it increasingly difficult to distinguish between **genuine communications** and **fraudulent attempts**. Impersonation fraud can target individuals, businesses or even government entities, often leading to **significant financial losses or data breaches**.

## Who:

the impersonation of executives

C-suite executives, particularly CEOs and CFOs, are the most common targets of deepfakes.

## How:

A plausible story through multi-layered, multi-factored fraud

Fraudsters use deepfake technology to mimic the voices or appearances of executives, often using deepfakes to target junior staff or those less familiar with the executive to manipulate them into circumventing controls.

Fraudsters combine deepfakes with traditional phishing techniques or social engineering. For example:

- Targeted attacks are often initiated using WhatsApp, before moving to deepfake video calls.
- Fake voice notes or video calls are often paired with phishing emails to create the pretence of multi-factored authentication.
- Fraudsters exploit the lack of cross-verification during remote interactions, especially in virtual meetings and voice calls.

## The number of deepfake attacks in the corporate world has recently escalated

A series of sophisticated **impersonation frauds rocked multiple industries** worldwide, showcasing the alarming capabilities of advanced deepfake technology and social engineering tactics.

Cybercriminals **manipulated digital communications** to defraud multinational corporations across a wide variety of economic sectors, resulting in losses in the millions. The various reported and unreported losses across all affected businesses, highlighting the **severe financial impact of these sophisticated impersonation frauds.**

# The scam strategy

### 1. Preparation and intelligence gathering:

Fraudsters meticulously gather publicly available information about the company's local CEO and CFO. This includes video footage from interviews, voice recordings from earlier calls and personal details from the company's website and the senior executives' social media profiles.

### 2. Technology preparation:

Using the collected data, criminals employ advanced AI algorithms to create convincing deepfake videos and voice clones of the CEO. They also develop fake email accounts and messaging profiles that closely mimic those of the executive team.

### 3. Trust building:

Scammers send an email to a mid-level finance manager, seemingly from the CEO's assistant. This mentions an upcoming confidential project and is loosely based on current events within the organisation. This initial contact was designed to establish credibility without raising immediate suspicion and is usually followed by a request to sign a non-disclosure agreement. Over the next few days, the fraudsters exchange several emails with the finance manager, providing believable details about the supposed project and gradually building trust. Bad actors also pretend to be real consultants or external lawyers from reputable firms – which adds to credibility of the storyline.

### 4. Voice cloning:

Once a foundation of trust is established, the scammers arrange a voice call between the finance manager and the 'CEO' using their AI-generated voice clone. During this call, the fake CEO discussed the urgency of a highly confidential acquisition.

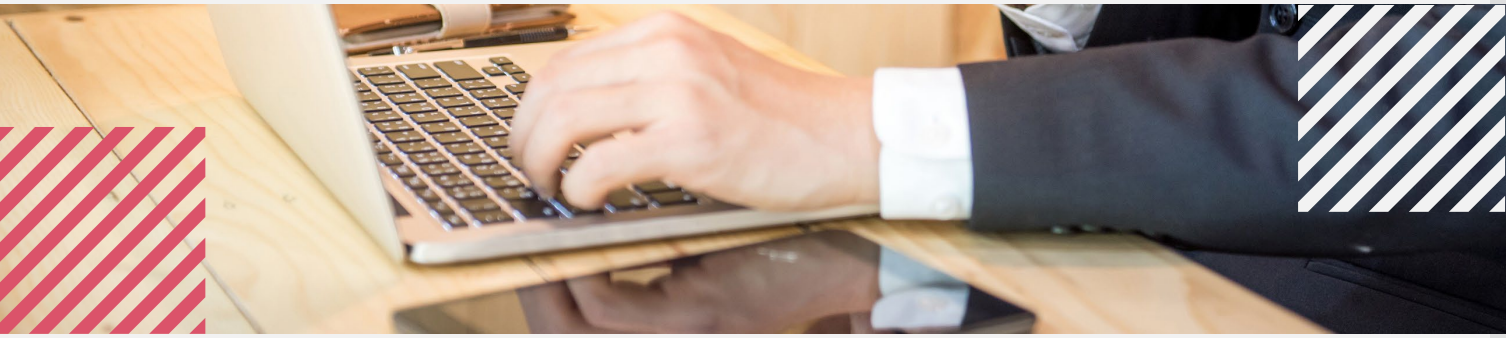
### 5. Video conference deception:

The fraudsters hold a fake video call, pretending to be the CEO and CFO, to discuss the secret deal and stress the need for non-disclosure.

### 6. Fund transfer request:

With trust and urgency in place, the fraudsters request the transfer of a substantial sum to a specified account, ostensibly to secure the acquisition deal

We see a number of deep fake cases where professionals are left scratching their heads over how this fraud could have occurred despite all the controls and safeguards being in place. Hindsight can be a great thing – but the fact is, this is happening, and **organisations are having to learn the hard way**.



Naturally, reported cases are only the tip of the iceberg. There are unreported cases and cases where fraudsters are unsuccessful due to **the strength of controls** and **vigilant staff**.

## If you are a victim of an impersonation fraud, what do you need to do?

**You need to act fast.** Questions a company should be asking itself in the event of falling victim to impersonation fraud are:

- How did the fraudster attain confidential information that was used against the company?
- Was anyone within the company involved in the fraud?
- Which security measures failed or were missing, and how can the company ensure this type of fraud does not happen again?

# Key essential steps to take by management in response to an attack

| | |
|---|---|
| **Step 1** | **Immediate Response:**<br>• Isolate the incident by taking steps to limit the spread and influence of it (e.g., work with your bank to block transfers and/or initiate tracing of funds for transfers that could not be blocked). |
| **Step 2** | **Investigate and assess:**<br>• Assess the scope and determine the extent of the breach.<br>• Conduct a forensic/cyber investigation that includes interviews, corporate intelligence, e-discovery, transactional analysis, review of logs and any other appropriate measures.<br>• Analyse the nature of the attack, identify vulnerabilities and suspects and understand how the impersonation occurred.<br>• Determine the extent of the breach, including which systems, data, and accounts have been compromised. |
| **Step 3** | **Recovery:**<br>• Tracking where the monies were transferred and seek legal options for recovery.<br>• Assess whether this is an insured event according to your insurance policy. |
| **Step 4** | **Remediation:**<br>• Limit the damage, remove the threat and restore normal operations.<br>• Set up systems monitoring for any signs of residual malicious activity.<br>• Enhance controls that may have failed and provide training to team members.<br>• Recover any lost or compromised data from backups. |

# Examples of remediation actions

| | |
|---|---|
| **People** | • Create a **culture of scepticism** by encouraging employees to question unusual emails / calls / messages.<br>• **Raise employees' vigilance** by updating them on latest scams to avoid the "this only happens to others" mindset.<br>• Organise **trainings and regular reminders.** |
| **Controls** | • Strengthen **controls around finance and payment processes.**<br>• Consider stricter controls for onboarding of new third parties and payments to new bank accounts.<br>• Layer **additional verifications** for sensitive transactions (e.g., call backs, identity checks). |
| **Cyber** | • **Protect against cyberattacks** by installing anti-virus, anti-spyware / malware monitoring tools and keep them updated.<br>• Deploy advanced anti-phishing gateways, real-time URL and attachment analysis.<br>• Domain watch service to block look alike domains<br>• Multi-factor authentication (MFA) to limit account / credentials compromise. |
| **Security** | • **Minimise sensitive information** that is available on executives online.<br>• Consider removing work emails, phone numbers from public domains.<br>• Avoid mentioning future whereabouts of company executives. |

# How can you defend your organisation from impersonation fraud?

## Impersonation risk assessment

- **Threat analysis and identification:** Conduct thorough analysis of past incidents, industry trends and potential threat actors. Evaluate the likelihood of impersonation attempts by reviewing access points, communication channels, and user interfaces that could be exploited.
- **Vulnerability Assessment:** Comprehensively review of your organisation's systems, processes and controls to identify any potential weaknesses.
- Perform data due diligence by **review publicly available information** on the key management and the company (particularly audio/voice data).

## Cybersecurity crisis readiness and management

- **Incidents inevitably happen –** and if not responded to properly they lead to crisis with a potentially devastating impact.
- **Incident Response Readiness:** Review of your organisation's procedures aimed at incident response & crisis management, conduct readiness exercise to practice in safe.
- **Crisis Management, Incident Response & Resilience:** Activate the prepared plans, gain control of the incident to contain damage and proceed to eradication of threats and returning to normal in a resilient way.

## Awareness training

- **Awareness training/workshops on deepfake technologies** can be organised as part of in-house training or conferences.
- **Increased awareness** should give employees the knowledge that media content can be faked. This is aimed at improving organisational security and mitigating security risks, as well as increasing awareness.
- **Preventing fraud:** It is important that employees understand how deepfakes are made and learn how to recognise deepfakes.

**Discover how we can support your organisation to defend itself against impersonation fraud.**

## Discover how we can support your organisation to defend itself against impersonation fraud

## Contact us




**Daniel Fu**

Partner, Forensics and Forensic Technology services

Mobile: +65 9627 4568

Email: daniel.j.fu@pwc.com



**Dmitry Kosarev**

Director, Forensics and Dispute Advisory services

Mobile: +65 9671 1326

Email: dmitry.kosarev@pwc.com



**Ankur Agrawal**

Director, Forensics

Mobile: +65 9623 9419

Email: ankur.b.agrawal@pwc.com


www.pwc.com/sg/en/services/risk.html