Lawley

CASE STUDY

Provided by Lawley

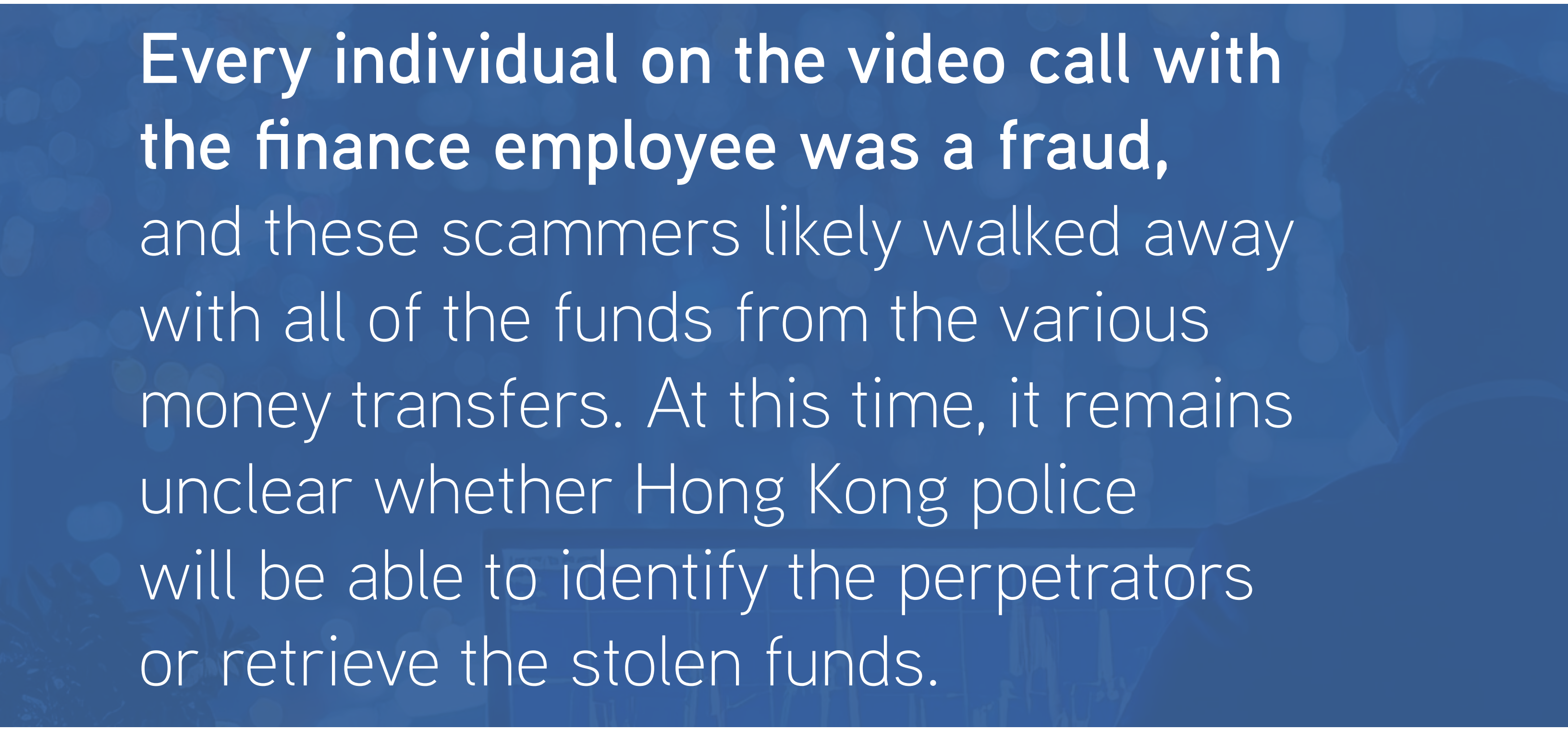
$25 Million Deepfake Scam Sends a Wake-up Call to Corporate Cybersecurity

In January 2024, a cyber incident involving deepfakes—technology that typically utilizes artificial intelligence (AI) to analyze existing images, videos and audio recordings of an individual to generate sophisticated forgeries of the person's likeness—resulted in the manipulation of a Hong Kong-based finance professional at multinational engineering firm Arup into wiring a considerable amount of company funds to fraudsters.

According to Hong Kong police, the finance employee initially received an email from an account claiming to be Arup's chief financial officer (CFO) and requesting the deployment of multiple confidential transactions. The employee suspected the email was a phishing scam, but he reportedly felt more at ease after joining a video call with individuals who looked and sounded like the CFO and several of his colleagues.

On this call, the employee was again asked to conduct a series of money transfers using company funds. Convinced he was communicating with trusted members of the firm, the employee moved forward with the transactions, ultimately making 15 total transfers to five separate bank accounts. The transactions totaled **200 million Hong Kong dollars,** which is equivalent to roughly $25.6 million in the United States.

The finance professional didn't realize he had been tricked until he discussed the matter with Arup's head office afterward. From there, the incident was reported to the authorities. Upon investigation, Hong Kong police determined that the perpetrators developed AI-generated deepfakes of the finance worker's CFO and colleagues by leveraging existing video and audio files of these individuals from online conferences and virtual company meetings.



Every individual on the video call with the finance employee was a fraud, and these scammers likely walked away with all of the funds from the various money transfers. At this time, it remains unclear whether Hong Kong police will be able to identify the perpetrators or retrieve the stolen funds.

This incident showcases the escalating severity of deepfake scams and other AI-related cyberattacks, which have become increasingly prevalent for businesses across industry lines. As such, it's important for businesses to be aware of notable deepfake scams and take steps to prevent similar incidents. In doing so, businesses can better safeguard critical funds and assets, minimize related disruptions and protect their own operations against large-scale losses.

This document explains the growing threat of deepfake scams, outlines other incidents involving such technology and their ramifications, and highlights associated risk management measures for businesses to consider.

Deepfake Risks on the Rise

The incident at Arup is just one example of a much larger trend. The past few years have seen a surge in deepfake scams, primarily due to evolving technology and the widespread adoption of AI tools. These advancements have allowed many cybercriminals—even those who lack technical expertise—to launch sophisticated attacks with ease and rely on deepfakes to enhance existing social engineering techniques (e.g., phishing and business email compromise scams), causing serious damage to affected businesses. Besides impersonating corporate executives in virtual meetings, other examples of deepfake scams include cloning employees' and vendors' voices in phone calls and generating fraudulent business documents and written communications. Deepfakes can be utilized to deceive both internal and external parties, compounding the potential scale of related attacks.

According to recent research from global technology company Entrust, incidents involving deepfake phishing and fraud have **skyrocketed by 3,000% since 2022,** with a deepfake attempt occurring every five minutes in 2024.

Furthermore, a survey conducted by international software firm Medius revealed that over half (53%) of businesses polled across the United States and the United Kingdom have been targeted in deepfake scams, while 85% of corporate executives view such incidents as an "existential" threat to their companies' financial security. What's worse, these scams are only expected to continue rising in the coming years.

Analyses from multiple industry experts anticipate that the deepfake market will reach **$13.9 billion in 2032,** up from $536.6 million in 2023.

Altogether, deepfake scams can significantly strain affected companies' operations, contributing to major disruptions, financial losses, eroded stakeholder trust, legal liabilities and lasting reputational damage. Nevertheless, a concerning proportion of businesses remain unprotected against these scams. According to a new report published by global IT security company LevelBlue, less than one-third (32%) of corporate executives believe their businesses are equipped to handle deepfake incidents, even though 44% expect them in the year ahead.

Considering these findings, it's evident that businesses simply can't afford to ignore deepfake risks.

Other Incidents Involving Deepfakes

In addition to the recent incident impacting Arup, many individuals and organizations have experienced deepfake scams over the years, emphasizing their growing prevalence and severity. Here are some of the most noteworthy incidents and their related ramifications:

Energy firm fraud—In March 2019, cybercriminals leveraged a fake audio clip to manipulate the CEO of an unnamed international energy firm into conducting a sizeable wire transfer. The fraudsters used publicly available audio recordings of the CEO of the energy firm's parent company to launch the deepfake scam, calling the firm's leader and asking them to send a large sum to a seemingly legitimate supplier. Believing they were communicating with the parent company's CEO, the firm's leader completed the transfer. The cybercriminals then promptly dispersed the stolen funds—totaling $243,000—to accounts across several different countries. Afterward, the fraudsters attempted to trick the firm's leader into issuing two more transfers, but these requests were met with growing suspicion and made the executive realize they had been scammed. Unfortunately, the stolen funds were never recovered. This incident was one of the first large-scale deepfake scams to impact a business, paving the way for future AI-related attacks going forward.

High school principal scam—In January 2024, an audio clip that sounded like the voice of Eric Eiswert, the then-principal of a high school located in a suburb near Baltimore, began circulating online. The clip, which appeared to be a "secret recording" of Eiswert making a series of derogatory comments about his school's students and staff, including racial and antisemitic remarks, quickly gained traction across different social media platforms. The clip generated uproar from the local community and beyond, with people across the country criticizing the principal and, in severe cases, sending him death threats. The school district eventually responded by putting Eiswert on administrative leave and conducting an official investigation of the clip. With assistance from the Baltimore Police Department, the district discovered that the clip was actually a deepfake made by the school's then-athletic director, Dazhon Darien. The clip was intended to be Darien's "revenge" against Eiswert for having him investigated for stealing from the school and causing other "work performance challenges." Darien was arrested and charged with creating and distributing the fraudulent clip, but the damage had already been done. Eiswert continued to receive harsh criticism online from those who still believed the clip to be real and faced ongoing security concerns, forcing him to take a new job in a different school. This incident showcased the lasting reputational damage that can accompany a deepfake scam.

Advertising agency attempt—In May 2024, cybercriminals created a fake WhatsApp account with publicly available images of Mark Read, the CEO of advertising firm WPP, and used this account to send out a virtual meeting invitation to another firm executive. During the meeting, the fraudsters leveraged online video and audio footage to establish a convincing deepfake of Read and attempt to trick the other executive into launching a “new business” that would require them to send corporate funding and disclose their personal information. Fortunately, the executive was suspicious of the interaction and didn’t comply with the cybercriminals’ request. Although the incident didn’t cause any damage to WPP, it highlighted the elaborate nature of deepfake scams and the importance of being skeptical of business communications involving unexpected requests or transactions.

City crosswalk incident—In April 2025, hackers compromised several crosswalk speakers across Seattle by swapping their standard voice commands with deepfaked audio clips of Jeff Bezos, the CEO of major online retailer Amazon. Instead of hearing the usual “wait” or “walk” commands upon pressing the impacted crosswalks’ buttons, pedestrians were met with Bezos’ cloned voice, asking them to “please, please don’t tax the rich.” The Seattle Department of Transportation fixed the affected crosswalks within a matter of days and promptly issued a statement condemning the incident, voicing concern that the cybercriminals responsible would be willing to “disregard the safety of people to make a political statement,” particularly those with vision problems who rely on crosswalk speakers to avoid road hazards. This incident shed light on the possible dangers and disruptions that can occur when deepfake scams affect community infrastructure.

Risk Management Considerations

Although the specific details of the aforementioned deepfake scams vary, these incidents all have at least one shared component: They stem from cybercriminals exploiting the target's security weaknesses. With this in mind, it's crucial for businesses to implement adequate risk management measures to avoid deepfake scams. There are several steps that businesses can take to deter cybercriminals and minimize such incidents, including the following:

Train employees. Employee training is critical to minimize the risks of deepfakes and associated damage. After all, employees are often the first line of defense against cyberattacks. Staff should be routinely educated on deepfakes, including what this technology is and how it may be used against businesses. By simply raising awareness of deepfakes, employees will be better equipped to spot them, allowing businesses to respond quickly and effectively to possible incidents.

Utilize detection software. While AI tools can be used to make deepfakes more convincing, this software can also be leveraged to help detect and mitigate potential deepfakes. In fact, large corporations such as Facebook and Microsoft use AI tools and similar software to identify and remove deepfake videos from their platforms. When it comes to deepfakes, the earlier these scams can be detected, the better; this allows businesses to act quickly and reduce related harm.

Establish response strategies. If and when businesses become targeted in deepfake scams, it's crucial to have proper response strategies that center around crisis mitigation and loss control. This includes outlining individual responsibilities, determining escalation practices and communicating appropriate response protocols. Additionally, if businesses haven't already, they should be sure to include deepfake scenarios in their cyber incident response plans.

Consult the experts. Businesses don't have to navigate their deepfake exposures alone. They should form strong relationships with local authorities, cybersecurity experts and industry groups to receive tailored guidance and assistance in managing their particular risks. These experts can also provide businesses with updates on recent deepfake incidents and other concerning cybersecurity trends, offering insight into managing emerging scams and preventing similar losses.

Secure ample coverage. On top of implementing effective risk management tactics, businesses should contact trusted insurance professionals to explore different coverage options that can help mitigate the financial fallout from deepfake scams. Possible policies to consider include commercial crime and cyber insurance. When securing such coverage, businesses should confirm that their policies apply to different deepfake scenarios (e.g., incidents involving spoofed images, audio and video footage) and other AI-related attacks. It's also imperative for businesses to review and update their insurance selections frequently, making sure these policies include adequate coverage limits.

Conclusion

As evidenced by the incident involving Arup and similar scams, deepfakes and other AI-related cyberthreats pose several risks for businesses. By reviewing these exposures, businesses can better understand the potential ramifications of deepfake scams and implement necessary risk management measures to help prevent them, ultimately protecting their operations while limiting major losses. Yet, even with these measures in place, deepfake incidents may still occur. In such cases, having sufficient insurance coverage can provide businesses with much-needed financial protection for the associated losses.

Contact us today for more risk management guidance and coverage solutions.

This document is not intended to be exhaustive, nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.