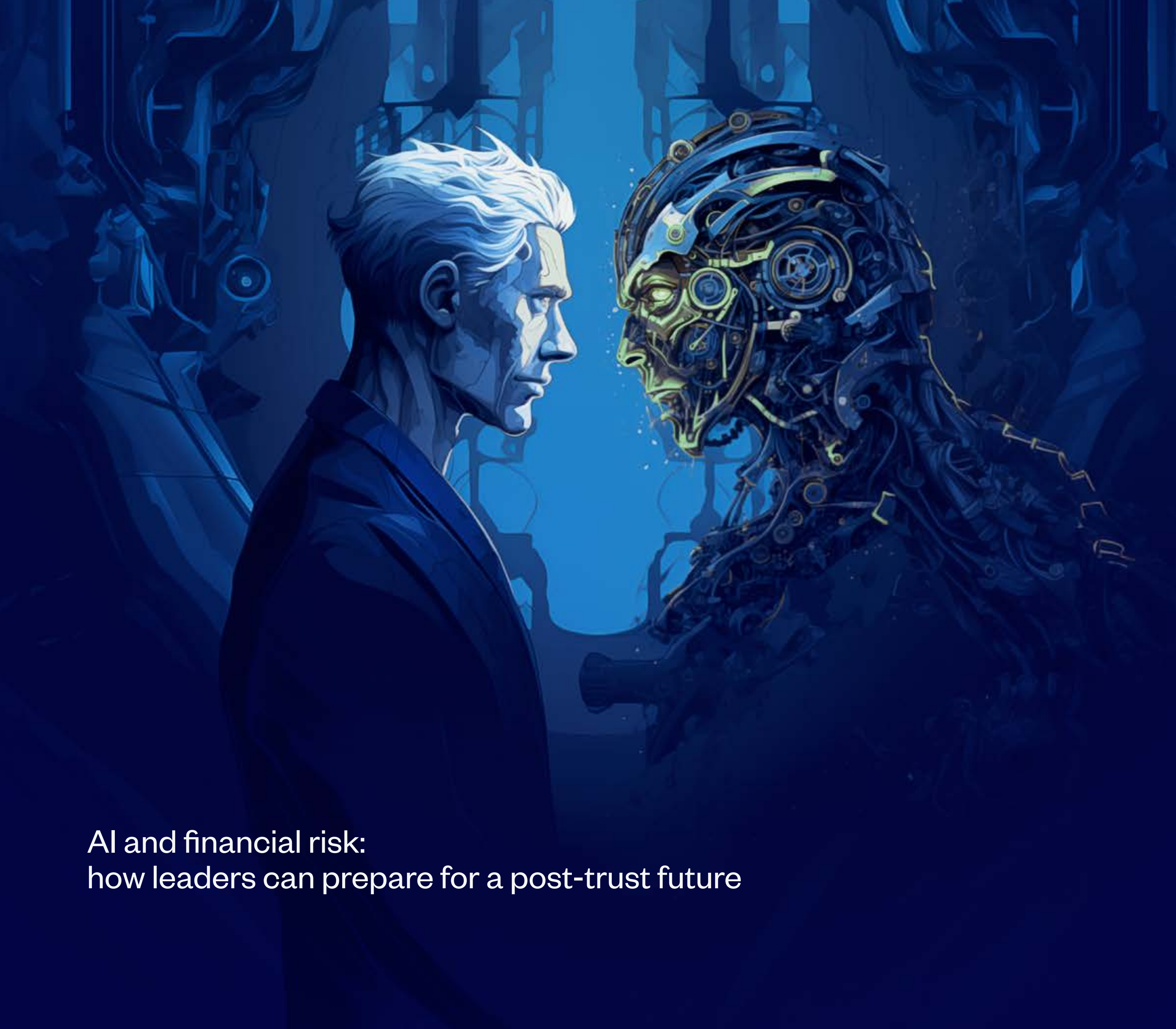
eftsure

Cybersecurity Guide for CFOs

2024 7th ed.



AI and financial risk:
how leaders can prepare for a post-trust future

Contents

Foreword 3

I. The current threat landscape 5

Understanding business email compromise (BEC) 6

How finance leaders see the threat landscape 8

II. Generative artificial intelligence (AI) 11

Breaking down AI and machine learning 12

What is generative AI? 13

Deepfakes 14

A new arsenal for scammers 14

III. Generative AI's role in scams 16

1. Chatbots and LLMs 17

    Malicious LLMs and chatbots 19

    Infiltration and attack strategies 20

2. Synthetic media and impersonation 21

    Audio and voices 21

    Video and faces 22

3. The unknown 23

    Risks in existing control procedures 24

    Risks in human behaviour and reasoning 25

IIII. Taking back control in an AI-powered world 26

Develop and drive a unified cybercrime strategy 27

Strengthen anti-fraud controls 27

Routinely pressure-test your controls 28

Double down on security hygiene 29

Develop and incorporate a synthetic media incident response 30

Additional resources 32

Foreword

In last year's edition, we asked this question: despite ballooning security budgets and closer scrutiny, why are so many business communities still seeing unprecedented losses to scams and cybercrime?

This year, the proliferation of generative artificial intelligence (AI) has created perhaps an even more urgent question: if businesses were already facing unprecedented cyber losses, how will they fare now that AI is equipping cybercriminals with powerful capabilities and rearranging notions of evidence and truth? This guide attempts to answer that question by examining generative AI and its impacts on the current threat landscape for AP and finance teams – as well as the novel, uncharted threats that are already looming on the horizon.

There's a lot we don't yet know about generative AI, but what we do know is that its pace of evolution is already outstripping laws, regulations and societal norms. Are finance leaders prepared for a post-trust future?

Mark Chazan
Chief Executive Officer
Eftsure

AI is shifting the paradigm of cybercrime ...and businesses were already losing millions.

I. The current threat landscape

Even without the scalability and potential of artificial intelligence (AI) tools, the rate of cyber incidents was already growing worldwide.

Global cybercrime costs are expected to grow by 15% per year, reaching

$10.5 billion USD annually by 2025.[1]

Australian businesses lost

$224 million AUD

to payment redirection schemes in 2022, according to the ACCC.

The number of attacks in Australia is growing year-on-year, with a

73% increase

in reported business scams last year. [2]

New Zealand scam reports are ticking upwards, with a

23% increase

from Q4 2023 and a

66% increase

in financial losses [3]

This data only tells part of the story, though – incidents are likely underreported and the lasting effects on a business are often underestimated. For example, the $224 million reported losses in Australia only include incidents reported to Scamwatch, ReportCyber and the AFCX. Eftsure survey data indicates that there is no primary reporting authority according to most financial leaders, with more than one in four saying they weren't sure whether fraud incidents were reported at all.[4]

1 Cybersecurity Ventures (October 2022). 2022 Official Cybercrime Report. Available at: www.esentire.com
2 Australian Competition and Consumer Commission (April 2023). Targeting scams: report of the ACCC on scams activity 2022. Available at: www.accc.gov.au
3 CERT NZ (June 2023). Cyber Security Insights Report. Available at: www.cert.govt.nz
4 Eftsure (October 2023). The State of Cyber Fraud Defence. Available at: www.eftsure.com

Understanding business email compromise (BEC)

According to 2023 data from the Australian Competition and Consumer Commission (ACCC), the largest losses for businesses were a result of payment redirection schemes, also called business email compromise (BEC) attacks.[2] In this type of attack, scammers infiltrate and weaponise email accounts to manipulate an accounts payable (AP) officer into making a fraudulent payment.

For instance, a threat actor might gain access to the email systems of one of your suppliers. From there, they can persuade your organisation's employees to change payment details or make a fraudulent payment into the threat actor's account. Even if your own cybersecurity defences are strong, the attack leverages weaknesses elsewhere in the supply chain and capitalises on human error.

---

[2] Australian Competition and Consumer Commission (April 2023). Targeting scams: report of the ACCC on scams activity 2022. Available at: www.accc.gov.au

This vulnerability is significant because banks don't reconcile the names of the recipients to the account and bank state branch (BSB) number.

On the ground: BEC tactics

Eftsure has seen a rise in increasingly hard-to-detect BEC tactics, including malicious actors gaining access to the email systems of both the target organisation and their supplier organisation. This way, the actor can orchestrate entire communication chains between executives at each company, making it easier to deceive AP staff into following instructions from an impersonated executive or supplier.

Despite the prevalence and growing sophistication of BECs, Eftsure data reveals that many organisations are foregoing the controls that tend to be more effective in thwarting BEC attacks.[4]

Segregation of duties

Ensures that no single employee has total control over any process, mitigating risks of fraud and error

Used by only 59%

Verbal verifications (call-back controls)

Verbally confirming bank details with a supplier before authorising an EFT payment, which reduces fraud risks even if a scammer has breached a supplier's email account

Used by only 46%

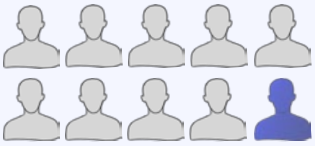
---

[4] Eftsure (October 2023). The State of Cyber Fraud Defence. Available at: www.eftsure.com

How finance leaders see the threat landscape

Eftsure's data shows that finance leaders are aware of broader cyber threats, even though specific anti-fraud controls aren't always tailored to cyber threats like BECs.

98% of CFO's



9 in 10*

Feel cyber-crime is increasing globally

82%

are very concerned about incidents like those at Medibank or Latitude Financial

1/2

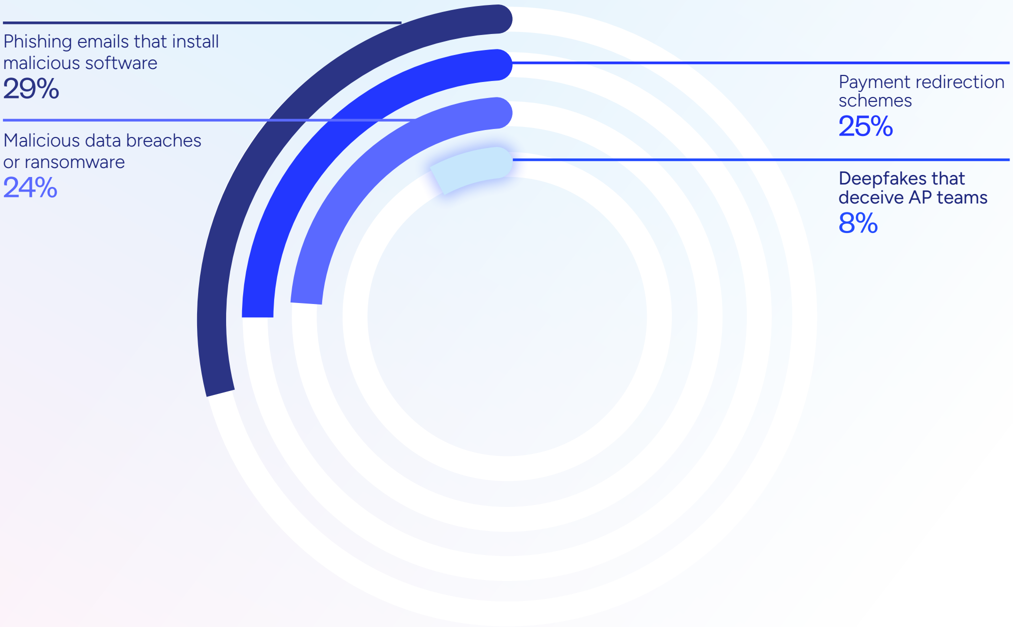
say business payment security concerns are higher compared to last year

Notably, respondents' broader concerns about global cybercrime tend to soften once they're asked about fraud risks within their organisations, and many do not rank deepfake audio or video (AI-generated synthetic media that imitates real faces or voices) as major threats.

60%

say they're concerned about cybercrime going undetected in their business

Biggest perceived cyber threats



The bottom line: even without the rapid technological advances we saw in 2023, finance teams were vulnerable to common cyber attacks and digital fraud tactics. Where does that leave finance teams now that those technological advances are accelerating?

> “From my point of view, if you don’t take AI seriously, if you don’t take cybersecurity seriously... then I don’t believe you’ll be here in the next five years.
>
> – Bastien Treptel,
> co-founder of CTRL Group[5]

---

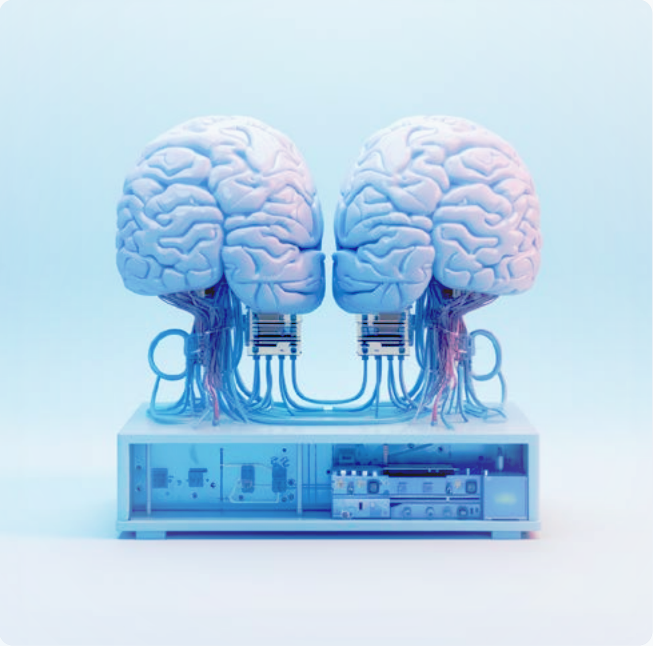
[5] SXSW Sydney (October 2023). “The rise of AI in cybersecurity”

II. Generative artificial intelligence (AI)

In early 2023, OpenAI's ChatGPT became the world's fastest-growing consumer application in history, amassing 100 million users in only two months.[6] Other generative AI companies attracted similar crowds of users and massive investments from some of the world's biggest tech companies, while each model catalysed a flurry of iterations built for specialised use cases.

There are now multiple, fast-expanding ecosystems of generative AI tools. Some leaders have heralded the fast evolution and widespread accessibility as a transformative technological revolution, while others have warned of unpredictable, irrevocable changes to all of society and even the fate of humanity.

[6] Hu, Krystal (March 2023). "ChatGPT sets record for fastest-growing user base." Available at: reuters.com



Breaking down AI and machine learning

Let’s start somewhere smaller than the fate of humanity – namely, what we mean when we talk about **AI**. AI is a broad field that aims to create systems capable of performing tasks that typically require human intelligence. These tasks include – but aren’t limited to – understanding natural language, recognising patterns, solving problems and making decisions.

Machine learning is a subset of AI that develops how computers learn and make predictions or decisions based on data. Instead of being explicitly programmed to perform a specific task, these algorithms use statistical techniques to learn patterns in data.

Examples of AI

- Rule-based expert systems that help diagnose diseases based on symptoms
- Natural language processing systems like chatbots or translation tools
- Computer vision systems that can detect and identify objects in images

What is generative AI?

Generative AI is a subset of AI, often using machine learning techniques, that focuses on generating new content. Where it's distinct from other forms of AI is that it generates content like text, images or sound – content that is entirely new and was not part of the original dataset used for training.

How does it work? Generative AI uses neural networks, which essentially teach machines to process data similarly to human brains. Two neural networks can form a generative adversarial network (GAN), in which one network generates new data and the other network assesses the quality of that data.

These two networks build off one another, continuously refining the generator network's output based on feedback from the other network.

This content generation can span multiple modalities and techniques. Large language models (LLMs) are a subset of generative AI specifically focused on generating and understanding text. LLMs are trained on vast amounts of textual data, enabling them to predict and generate human language.

AI-generated images of the pope, created through Midjourney.
Source: reddit.com

Examples include OpenAI's GPT series (like GPT-3 or GPT-4) and BERT by Google. While all LLMs are generative AI when used to produce text, not all generative AI systems are LLMs, as many generate non-textual content.

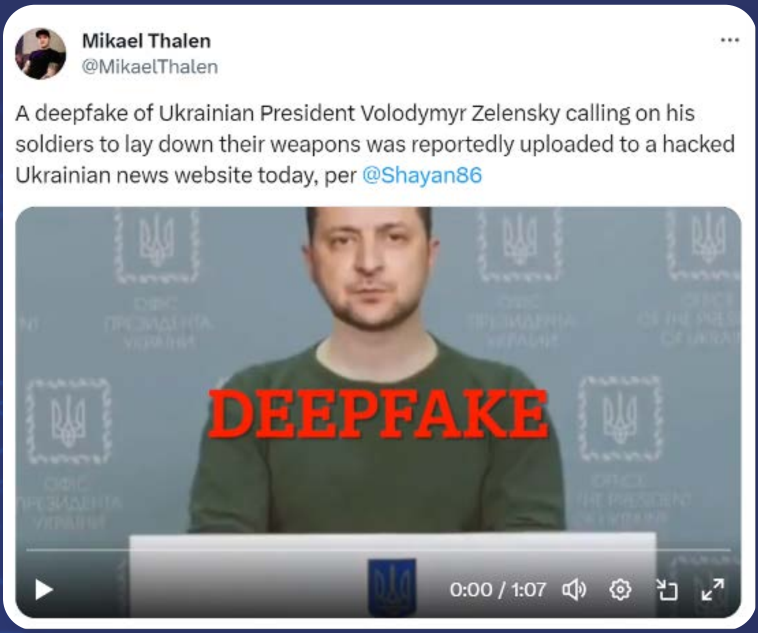
Types of generative AI

- Text generation, like **ChatGPT** or **Bard**
- Image generation, like **DALL-E** or **Midjourney**
- Text-to-speech
- Style transformations

Deepfakes

Deepfakes refer to AI-generated synthetic media (video, audio or images) in which simulated ones replace the appearance of real people.

While GANs are frequently used to create deepfakes, other neural network architectures can also be employed. Deepfakes involve training on a dataset of target videos to replace one person's likeness with another's, often leading to highly convincing, fabricated media.



Mikael Thalen
@MikaelThalen

A deepfake of Ukrainian President Volodymyr Zelensky calling on his soldiers to lay down their weapons was reportedly uploaded to a hacked Ukrainian news website today, per @Shayan86

X users share a known deepfake of Ukrainian president Volodymyr Zelensky. Source: x.com

A new arsenal for scammers

Whether it's deepfake audio calls or polished-sounding phishing emails, broader access to generative AI tools has opened a new world of scalable attacks and synthetic media. In other words, scammers have a broader array of tools than ever.

But, to start building resilient and flexible defences now, finance leaders need to understand specific applications. The following section will examine how cybercriminals already use AI to circumvent financial controls – and what's next.

> “This is the year that all content-based verification breaks. And our institutions haven’t had time to catch up with this change.
>
> – Aza Raskin, co-founder of the Center for Humane Technology

---

7 Harris, Tristan, Raskin, Aza (June 2023). “The A.I. Dilemma.” Available at: www.aspenideas.org

III. Generative AI's role in scams

There's a wide range of positive, promising applications of generative AI: faster, more accurate diagnostics in healthcare, advanced manufacturing, more efficient and sustainable agriculture, safer and smarter digital cities, to name a few.

Even in the cybersecurity arena, specialists are already leveraging AI tools to protect organisations' systems and data. In October 2023, Commonwealth Bank's General Manager of Cyber Security, Andrew Pade, explained that security teams have been using generative AI to identify threats in real time and create deceptive technologies that act as honeypots for threat actors.[8]

However, AI is assisting both defenders and attackers. After all, cybercriminals have access to the same AI tools and technologies – and then some. Unlike governments and businesses that are bound by regulations, privacy rules or security restrictions, threat actors are unfettered in their use of both mainstream and black-market AI tools.

It's critical to understand how these capabilities can be used against finance professionals.

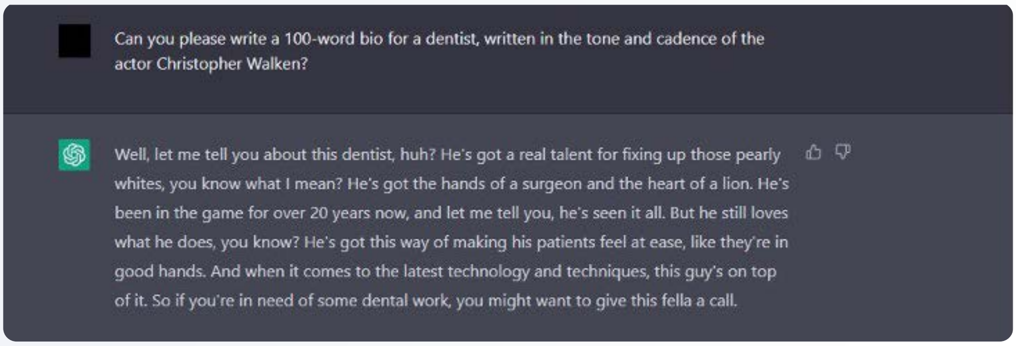
---

[8] SXSW Sydney, October 2023. "The rise of AI in cybersecurity"

1. Chatbots and LLMs

Cybercrime use cases: Refining BECs and phishing tactics, analysing large datasets, identifying vulnerabilities, developing malware and devising new attack strategies.

LLMs like ChatGPT are trained on vast amounts of text data. When prompted with user input, they generate coherent and contextually relevant text by predicting the next word in a sequence, leveraging their extensive training to serve information and conversational responses. They can act as on-demand virtual assistants, analyse spreadsheets or generate dentist bios in the voice of Christopher Walken.



Can you please write a 100-word bio for a dentist, written in the tone and cadence of the actor Christopher Walken?

Well, let me tell you about this dentist, huh? He's got a real talent for fixing up those pearly whites, you know what I mean? He's got the hands of a surgeon and the heart of a lion. He's been in the game for over 20 years now, and let me tell you, he's seen it all. But he still loves what he does, you know? He's got this way of making his patients feel at ease, like they're in good hands. And when it comes to the latest technology and techniques, this guy's on top of it. So if you're in need of some dental work, you might want to give this fella a call.

They're also helping threat actors perfect their cyber attacks. Grammatical mistakes are a common warning sign of a scam attempt, while impersonation attempts can be foiled by email wording that sounds unnatural or out-of-character. Now, mainstream AI tools like ChatGPT can help attackers sidestep these issues and create more polished, more effective phishing messages or BEC attacks.

For instance, Ryan Kalember – Vice President of Cybersecurity Strategy at email security company Proofpoint – has explained that LLMs are sparking major BEC upticks in markets that were previously off-limits due to language and cultural understanding barriers, such as Japan.

> "
>
> BECs used to be a contentious topic in Japan because the attacker did not speak Japanese and didn't understand business customs. Now the language and cultural understanding barriers [are] gone... and [attacks] are increasing in volume.
>
> **– Ryan Kalember, VP of Cybersecurity Strategy, Proofpoint [9]**

Kalember also points out potential AI use cases for a multi-persona phishing tactic explored by Proofpoint research, in which threat actors masquerade as different parties within a single message thread.[10] Leveraging the concept of social proof, this tactic uses benign, multi-persona conversations to win a target's trust and eventually persuade them to click on malicious links, give away sensitive information or process fraudulent payments.

Eftsure has previously flagged similar tactics in foiled fraud attempts, with attackers orchestrating back-and-forth 'conversations' after compromising the email systems of both the target organisation and supplier organisation. While the basic structure of a BEC attack or phishing attempt remains the same, AI tools are making these more advanced tactics easier and more scalable.

[9] Risky Business, July 2023. "Risky Biz Soap Box: BEC actors embrace LLMs to attack Japan." Available at: risky.biz

[10] Proofpoint, September 2022. "Look what you made me do: TA453 Uses Multi-Persona Impersonation to Capitalize on FOMO." Available at: www.proofpoint.com

Malicious LLMs and chatbots

> Some of the scarier tools are being birthed out of the dark web. You break into an email server, and then the AI goes and reads all the conversations and tells you how to best scam this organisation. I don't think Australian businesses are quite yet ready for that
>
> **– Bastien Treptel, co-founder of CTRL Group**[11]

Even heavily moderated AI tools like ChatGPT can give threat actors a crucial edge. Similar tools are spreading across black markets on the dark web, except these models are specifically designed to aid criminal activities and may be trained on datasets that include phishing messages and malware code.

WormGPT and FraudGPT are just a few examples of such tools. In July 2023, researchers from cybersecurity firm SlashNext uncovered the promotion of WormGPT as a "black hat alternative" to ChatGPT.[12] Within a week, other researchers sounded the alarm about a similar tool, FraudGPT, circulating in Telegram channels.[13]

Later in 2023, Kaspersky researchers found counterfeit websites peddling fake access to WormGPT, illustrating the growing popularity of the tool.[14]

[11] SXSW Sydney, October 2023. "The rise of AI in cybersecurity"

[12] Slashnext, July 2023. WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks. Available at: slashnext.com

[13] Netenrich, July 2023. FraudGPT: The Villain Avatar of ChatGPT. Available at: netenrich.com

[14] Kaspersky, September 2023. WormGPT-mimicking scams surface on the Darknet. Available at: kaspersky.com

Infiltration and attack strategies

AI assistance isn't just helping cybercriminals hone BECs or phishing messages, though. LLMs and other AI models can effectively act as super-assistants, crunching large datasets to find vulnerabilities, developing malicious code and brainstorming altogether new attack strategies. This is especially true for the black-market versions, which don't have the same guardrails or regulations as ChatGPT or Bard.

Threat actors can access ever-widening pools of ill-gotten personal data on the dark web, but AI capabilities help spot patterns in these datasets and whittle down shortlists of the most vulnerable targets. Just as ChatGPT can help you devise new marketing strategies or ideas for a child's birthday party, its malicious iterations can be used to brainstorm new approaches to infiltrate or de-fraud organisations and individuals.

This isn't emerging technology or hypothetical risks – the threats are here, today. But there's a potentially even more challenging threat on the horizon: synthetic media.

2. Synthetic media and impersonation

Cybercrime use cases: Impersonating contacts, augmenting social engineering attacks, diminishing trust across partner organisations and value chains.

Massive losses result from deceptive tactics that take place entirely through text and email. The next frontier is deceptive tactics that use synthetic media, leveraging realistic faces and voices – or even the faces and voices of people you know.

Tracing synthetic media manipulation back to 2017 on an unsavoury adult Reddit forum, Queensland University of Technology researcher Lucas Whittaker and the co-authors of "Why managers should adopt a synthetic media incident response playbook in an age of falsity and synthetic" media explain how GANs can generate content to an "ultrarealistic standard."[15]

That paper details a variety of business risks stemming from weaponised synthetic media, including reputational, economic, security and operational risks.

Audio and voices

How scammers weaponise the voices of people we know and love

A CEO receives a call from someone posing as the boss of his parent company, in the leader's signature German accent and tone, instructing the CEO to transfer an immediate payment to one of their suppliers.[16] A mother receives a call from a supposed kidnapper who has taken her daughter and is demanding a ransom payment, while her daughter's voice pleads in the background.[17]

These aren't science fiction plotlines. These are real-life scams, one of which took place in 2019, well before the proliferation of generative AI had lowered the barriers to accessing voice conversion technology.

---

[15] Whittaker, Lucas, Kietzmann, Jan, Letheren, Kate, Mulcahy, Rory Francis, Russell-Bennett, Rebekah (2022). Brace yourself! Why Managers should adopt a Synthetic Media Incident Response Playbook in an Age of Falsity and Synthetic Media Business Horizons. Available at: www.sciencedirect.com

[16] The Wall Street Journal, August 2019. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. Available at: www.wsj.com

[17] ABC News (US), July 2023. Experts warn of rise in scammers using AI to mimic voices of loved ones in distress. Available at: abcnews.go.com

Whittaker tells Eftsure that scams like the 2019 incident with the German CEO are "just the beginning of an increasing trend of voice conversion scams."

"We're seeing increasingly widespread access to GAN-generated audio. Easily accessible voice cloning services generate pitch-perfect voice clones off of voice samples provided to the platform. [Multiple platforms] permit anyone to generate highly realistic speech audio from mere text input," says Whittaker.

"Lots of research focus is being placed on the development and optimisation of GAN models which specialise in vocal synthesis and conversion, so the synthetic voice output from openly available platforms will only become more realistic, expressive and seemingly human.

"Scammers are already using AI-facilitated voice conversion scams to target individuals globally and also here in Australia."

> All you need is a few seconds of someone's voice to create an imitation of them – given the increasing accessibility and sophistication of voice cloning tools and the vast amounts of rich audio content people post online, impersonation incidents are unfortunately going to become more common.
>
> **– Lucas Whittaker, QUT PhD candidate and deepfake researcher**

Video and faces

While there are fewer instances of scams that rely on synthetic video, it only took a few years for voice conversion scams to go from an outlier in the Wall Street Journal to a growing worldwide trend.

Finance leaders shouldn't dismiss this risk when considering future threats and how to protect against them. Geographic dispersion is a reality for many organisations, their partners and their supply chains, making video calls a standard – and trusted – channel for verifying information. The ubiquity of recorded video calls also creates a large pool of data for threat actors to leverage if systems are breached.

3. The unknown

Cybercrime use cases: Yet to be devised – or anticipated.

> Give a man a fish and you feed him for a day; teach a man to fish and you feed him for a lifetime. But teach an AI to fish and it'll teach itself biology, chemistry, oceanography, evolutionary theory and then fish all the fish to extinction
>
> **– Aza Raskin, co-founder of the Center for Humane Technology**[18]

The risks of synthetic media and LLMs are known. Threat actors are leveraging many of these capabilities right now, and it's not hard to see how emerging capabilities like synthetic video can augment existing BEC or social engineering tactics.

The third area of risk within generative AI is what we do not currently know. While some dismiss new AI capabilities as overhyped buzzwords, others are warning that we simply don't know where this technology might take us.

In the latter camp are Aza Raskin, co-founder of the Center for Humane Technology, and Tristan Harris, Executive Director. In their presentation "The AI Dilemma," they argue for greater international regulation of generative AI, noting that current models can learn skills that even their creators didn't anticipate.

"As we've talked to... AI researchers, what they tell us is that there is no way to know," Raskin said. "We do not have the technology to know what else is in these models."

Combined with the ultra-fast deployment of AI tools throughout the wider population, AI's self-strengthening capabilities cause advances to occur on a "double exponential curve." Harris and Raskin argue that the only way to ensure these advances don't cause unforeseen catastrophes is to upgrade "our 19th-century laws, our 19th-century institutions for the 21st century."

---

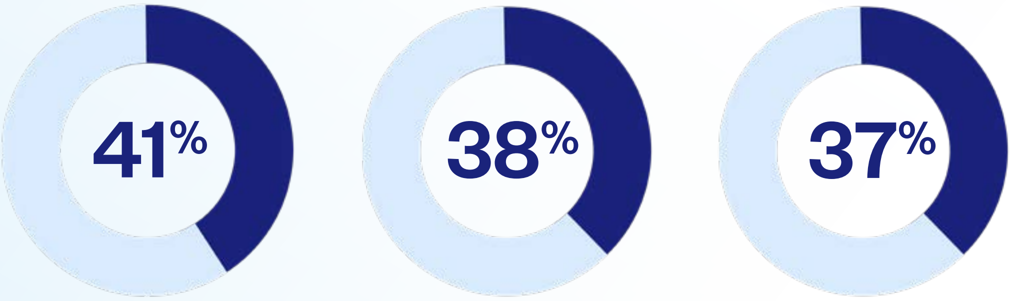
[18] Harris, Tristan, Raskin, Aza (June 2023). "The A.I. Dilemma." Available at: www.aspenideas.org

Risks in control procedures

Even without the threat of synthetic media, many organisations are skipping vital anti-fraud controls and processes, potentially raising their risks of falling victim to cyber scams.

Eftsure found that verbal verifications, which could help weed out scam attempts that leverage voice conversion, are only used by less than half of organisations. Even among those who deploy this control, large portions are skipping best-practice approaches – which means existing vulnerabilities are likely to become more pronounced as voice conversion scams rise.[19]

Among the 46% of survey respondents who use verbal verifications:



use independently sourced phone numbers

initiate calls via outbound lines

open-ended questions during calls, which can identify both human impersonators and synthetic media

---

[19] Eftsure (October 2023). The State of Cyber Fraud Defence. Available at: www.eftsure.com

Risks in human behaviour and reasoning

You might look at existing deepfakes and question whether you or your employee would find them convincing. Some examples have an 'uncanny valley' effect or look otherwise unnatural. However, not only are outputs likely to become increasingly realistic, but experts say our brains are wired to believe synthetic media.

It's already common for scammers to capitalise on employees' busy schedules or cognitive load. For instance, malicious actors will target skeleton staff or employees who are about to go on leave. Other time-honoured tactics include urgency and pressure, such as impersonating a senior executive and telling an employee that a major deal is contingent on processing the payment within the next hour.

Whittaker says synthetic media plays on several similar cognitive biases and mental shortcuts, which could make it even harder to counter these tactics.

Limited awareness of deepfake capabilities.
"A lot of people aren't aware of how realistic generative AI and deepfake generation can be," says Whittaker, a claim supported by Eftsure's survey data of finance professionals. "Those with limited awareness have no real cause to question synthetic content if it looks or sounds realistic enough. Deepfakes in particular can be deceptive given the richness of video content – we're less inclined to systematically appraise sources of richer information like video content as it looks more credible due to the fact it appears more realistic."

Familiarity heuristics.
"This is the tendency people have to trust people or objects they're familiar with. If an employee is presented with a voice or face they recognise, like a coworker's, their natural instinct is to trust the source of the information."

Confirmation biases.
Whittaker also explains that we tend to place more credence in evidence that is consistent with our prior beliefs and expectations. "If an attacker uses information the employee already knows or believes to be true, it can make the employee more inclined to trust the attacker."

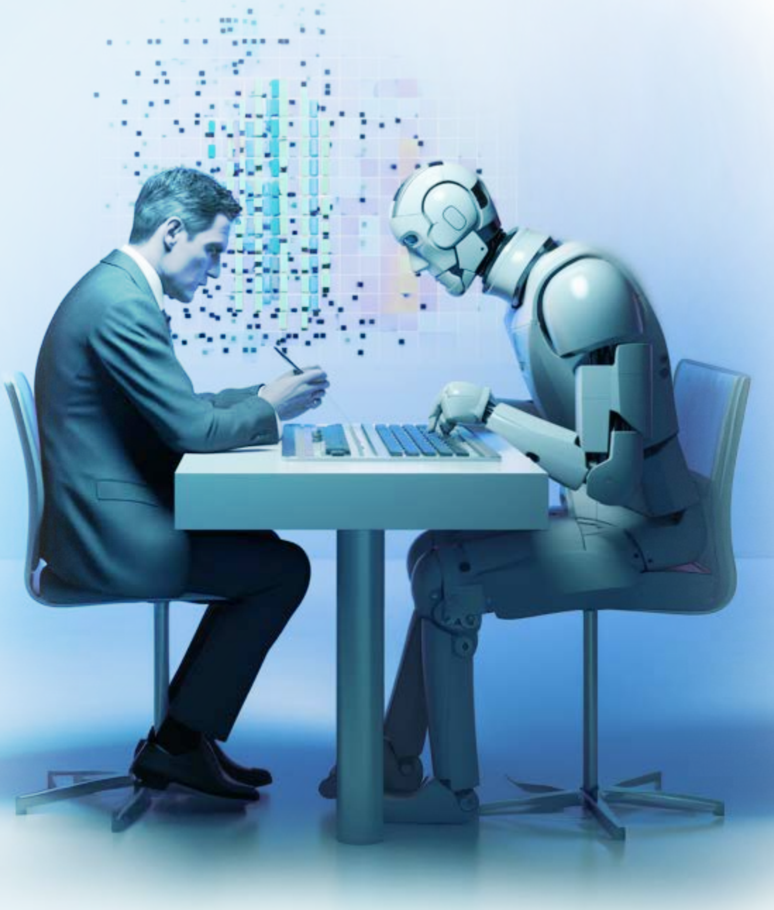
Authority biases.
"Employees are more inclined to follow the instructions of those in positions in authority, potentially without the legitimacy of these instructions being questioned." By imitating authority figures' faces or voices, attackers can harness this powerful bias and circumvent precautions that an employee might otherwise take.

IIII. Taking back control in an AI-powered world

CFOs face a three-fold risk:

1. Many organisations are not fully prepared for even basic scams or cyber attacks.
2. Generative AI capabilities are increasing the efficiency, reach and scale of existing scams and cyber attacks.
3. Most of today's controls and anti-fraud measures, no matter how robust, were not designed with AI-powered scams or synthetic media in mind.

To address all three, CFOs will need a multi-layered mix of solutions.



Develop and drive a unified cybercrime strategy

1/2

of organisations employ **training modules** developed with their IT or security teams

Less than half

have developed a **cybercrime strategy** with IT or security

According to Eftsure's 2023 survey data, only about half of finance leaders say they're aligning with technology specialists on training and strategy.

Even if you've already implemented a cybercrime strategy, most organisations will benefit from tighter alignment with cybersecurity practices and training. This strategy should encompass people, processes and technology.

Strengthen anti-fraud controls

Fortifying control procedures against today's scams is a good starting point for protecting against tomorrow's scams, too.

After all, when distilled into their most basic elements, most AI-enabled scams are still fundamentally the same BEC attacks or social engineering scams we've seen for decades – it's just that AI tools can increase their volume, scale and efficiency, while synthetic media can make old-fashioned fraud attempts even more convincing.

Control procedures like segregation of duties and call-back controls are some of the strongest defences against these scams. Standardising and automating parts of these processes helps ensure that staff don't cut corners, intentionally or unintentionally.

Routinely pressure-test your controls

Threat actors tend to be more organised and aware of internal processes than some leaders realise. This is especially true now that AI tools can help them more quickly parse large datasets and communications after they've infiltrated a system. As a result, even if you already have existing controls in place, they need to be continuously pressure-tested to see how they stand up against evolving cyber threats.

Cybersecurity specialists use a practice known as penetration testing, in which security experts simulate cyberattacks on a system to identify vulnerabilities before malicious hackers can exploit them. Within a finance function, this looks like pressure-testing various controls to identify where there might be gaps in the process – this testing should happen while keeping in mind the potential for AI-honed messages or synthetic media.

False authority

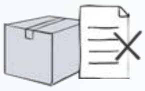
Use an email account belonging to your organisation's CEO or CFO. Send fictitious emails asking your AP team to urgently process payments.

False supplier

Use a spoofed supplier email account or a tester who phones the AP team, asking them to update the "supplier's" banking details.

Modified phone numbers

Send fake invoices to your AP team with manipulated phone numbers to see if current call-back controls are sufficient – and whether the team is adhering to them.



Undelivered goods

Send fake invoices for goods that were never ordered or delivered, helping you gauge your AP team's adherence to three-way matching.

Duplicate dupe invoices

Send multiple fake invoices to determine whether duplicate invoice checking is taking place.

Modified GST or ABN

Send fake invoices with false GST or ABN details to check whether regulatory compliance checking is taking place.

Double down on security hygiene

Implement multi-factor authentication (MFA) on all accounts whenever possible, and ensure passwords are never duplicated or shared. Passwords should also be complex and software should be patched regularly.

This is another area that calls for a unified cybercrime strategy, since you'll want to align with security professionals on training. Synthetic media risks and common fraud tactics should be learned alongside fundamental security hygiene, ensuring employees understand both the risks and how certain practices mitigate those risks.

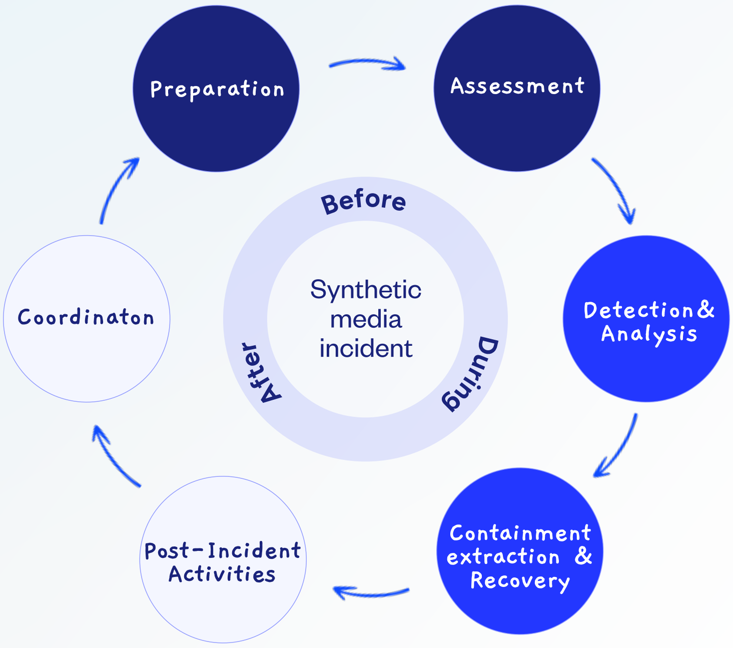
Leverage technology

Cybercriminals are already using technology to work smarter and faster – don't cede the advantage. The right technology solutions can help you scale and automate processes without sacrificing efficiency.

Look for solutions that can act as guardrails for critical steps like payment processing, especially those that integrate with your existing tech stack and help make employee experiences easier or more seamless. No solution or procedure will be a panacea, so opt for technology that facilitates resilience and adaptability.

Develop and incorporate a synthetic media incident response

QUT researchers have urged leaders to adopt a synthetic media response playbook, which involves six phases.[20]



Many of these components overlap with a cybercrime strategy – particularly those around training and assessing threats – which is why it's crucial to collaborate with leaders across the business to understand and protect against synthetic media risks.

---

[20] Whittaker, Lucas, Kietzmann, Jan, Letheren, Kate, Mulcahy, Rory Francis, Russell-Bennett, Rebekah (2022). Brace yourself! Why Managers should adopt a Synthetic Media Incident Response Playbook in an age of Falsity and Synthetic Media Business Horizons. Available at: www.sciencedirect.com

"Firstly, promoting synthetic media incident awareness is essential so the entire organisation is aware of the risks which are presented and the potential infrastructure and psychological vulnerabilities which could be taken advantage of," says Whittaker. "Training and awareness programs will be vital in establishing an organisational culture that understands the risks which synthetic media presents to their operations."

"A centralised synthetic media response strategy should be the goal of any organisation planning a response," explains Whittaker. "Enacting this strategy may manifest in different ways depending on various organisational departments. For example, finance could implement enhanced verification protocols such as biometric authentication or two-factor authentication when large or urgent financial transactions are required."

As part of the preparation and assessment phases, the playbook also includes mapping out your organisation's "crown jewels" and the assets most likely to attract threat actors, e.g. money.

"Many organisations already understand who has access to their crown jewels, so focusing on providing extra protections for the individuals and shoring up the authentication and approval processes associated with their roles could be a more effective investment of organisational resources," explains Whittaker.

> "
>
> It's paramount to boost the protection of those most at risk of being targeted. That might be through the provision of more extensive educational modules, providing them with devices that have greater in-built security protocols, or requiring more extensive levels of authentication when they need to undertake important actions.
>
> **– Lucas Whittaker, QUT PhD candidate and deepfake researcher**

[9] Risky Business, July 2023. "Risky Biz Soap Box: BEC actors embrace LLMs to attack Japan." Available at: risky.biz

Closing remarks

We don't currently know the full extent of AI's threats (or potential benefits), but we do know that we're entering a new era – one that will force us to reevaluate how we understand evidence and trust. We must learn to live and work in a world where AI is embedded into everyday life, which includes reassessing our security controls and strategies. Leaders can't ignore this – technologists and even AI researchers have already issued warnings about its malicious use and have advocated for ethical practices.

However, even with better international regulation of generative AI, finance leaders will still need to adapt to a new reality. After all, cybercriminals are not as bound by laws or regulations and will always look for ways to capitalise on new technology. To stay one step ahead of them, CFOs need to think creatively, stay informed and implement technology-driven processes

Additional resources

Cybercrime Strategy

Cybersecurity Guide for CFOs: 6th edition

Processes

Financial Controls Guide

Technology

Explore a dedicated B2B payment protection solution

eftsure

Technology is giving cybercriminals the upper hand.

Eftsure tilts the playing field back in your favour.

Request a demo

1300 985 967 | sales@eftsure.com.au
eftsure.com.au