

Sponsored Report



5 emerging business cyberthreats — and how to combat them

From deepfakes to payment fraud, companies are at risk of increasingly complex cyberthreats — with finance taking a leading role in mitigating risks.

By Stephen Lynch

Cybersecurity threats to business are becoming so sophisticated that even trained professionals are struggling to identify AI-generated deepfake impersonations, putting businesses at risk of advanced fraud and phishing attacks.

Cybercrime is also extremely costly. Cybersecurity Ventures' 2025 [annual report](#) estimates a global cost of around £7.7 trillion in 2025 — which would make it the world's third-largest economy if measured as a country's GDP.

Finance functions are increasingly targeted by these threats that aim to exploit both digital systems and human processes.

No business is too large or too small to be targeted. All that the criminals are hoping for is one weak spot or one employee in the loop to make a mistake.

EMERGING BUSINESS CYBERTHREATS

1. Deepfakes

While AI is driving efficiencies by enabling businesses to do things more easily than ever before, it's also being weaponised. Attackers are [using AI to conduct deepfake fraud](#) in video calls, where they impersonate executives or anyone who can authorise a payment. The goal is to fool finance people into making a money transfer.

Engineering company Arup was the victim of a [sophisticated deepfake attack](#) that impersonated its UK-based CFO to urgently request payments totalling \$25.5 million from a finance worker in Hong Kong. A quick-thinking Ferrari executive [averted a deepfake scam](#) when he asked the person purporting to be the company's CEO a question only the CEO would know. Unable to answer, the would-be scammer ended the phone call and spared the company a major financial loss and reputational damage.

Alarmingly, an executive talking on a phone call for only minutes is enough time for a criminal to take their voice imprint for impersonating.

2. Phishing

Phishing has been around for a long time.

Criminals use scam emails, text messages, or phone calls to trick victims into visiting a website or downloading a file that disguises a virus to steal financial details or other valuable information.

It's a classic tactic but also an emerging threat because it's becoming much more sophisticated and believable.

Phishing uses targeted information to catch the recipient's eye. Criminals understand, for example, that businesses will often jump at the opportunity to win a new contract, so they send a fake request-for-proposal (RFP) document containing malicious hyperlinks.

3. Ransomware

Ransomware is, in essence, a tool for malicious actors to extort money from an organisation. Unfortunately, it is also a third-party software and service available to purchase on the dark web — the purposely hidden part of the internet that's inaccessible through standard methods and browsers.

Jez Goldstone, startup founder and former Barclays Bank head of security architecture, cloud security, and cyber innovation, believes that, of all the emerging threats, ransomware presents one of the biggest challenges. Some ransomware techniques are indiscriminate. According to the UK's Information Commissioner's Office, the commonly used "scatter gun" style attack involves sending thousands of phishing emails with the aim of delivering ransomware to at least a single victim.

Other techniques, described by the global Financial Action Task Force, include "big game hunting", which is more targeted and precise. In this case, criminals select organisations they believe will want to avoid public scrutiny by paying a ransom or those with higher business downtime costs.

Data compiled by cyberthreat management platform NordStellar reveals that the number of ransomware attacks doubled in the first half of this year, with small and medium-size US firms being hit especially hard.

Goldstone said: "Many organisations think attackers aren't interested in focusing on them. But they [cybercriminals] don't [always] choose targets selectively."

He went on to explain: "Automated scanners are constantly scanning the internet to look for vulnerabilities and gaps in organisations' defences. So you don't have to be high-risk or special to get found out."

4. Payment fraud

AI is also being used to create convincing but fake invoices to defraud a business's accounts payable department. This typically involves changing the account number of an existing supplier, accompanied by legitimate-looking email trails.

This is a particular problem for businesses that don't control the processes and procedures of other businesses in their supply

chain. "Third-party risks have become critical, as attackers target less-secure vendors or outsourced finance platforms to gain access to internal systems or spoof legitimate requests," said cybersecurity expert Thomas Balogun, who is a UK Security Institute board member.

5. 5G and IoT technology

5G now connects the physical and virtual worlds in many ways, including autonomous vehicles, security cameras, and sensors. Some business leaders are particularly concerned because of how embedded 5G is within most mobile devices.

The technology is complex and developing, and so its threats are unique. Internet of Things (IoT) devices can be taken over for distributed-denial-of-service (DDoS) attacks — giving cyberattackers a broader range of targets that are more difficult to monitor and defend.

Undetected breaches often originate from compromised credentials and unprotected endpoints, as these are common points of entry. Once attackers gain access, long-term breaches can happen.

Other threats such as "cloud-jacking", where cybercriminals hack into a company's cloud environment, demonstrate how vulnerabilities enable both infiltration and persistent, hard-to-detect attacks across networks and systems.

SOCIAL ENGINEERING

These threats all share some common themes. One is the criminals' goal of infiltrating a business by any means necessary, frequently to manufacture a false sense of urgency and pressure so people rashly make payments under false pretences or coercion. This is the social engineering aspect that uses psychological manipulation to induce fear (for example, contacting family members to prey on emotions) or to keep the target locked into Type 1 thinking, where they are driven by emotions and past experiences to make intuitive decisions too quickly.

For Balogun, these nascent cyberthreats are not only more elaborate today, but also increasingly convergent "as AI enhances social engineering, which in turn exploits

About the author

Stephen Lynch is a freelance business writer. To comment on this report, contact Oliver Rowe at Oliver.Rowe@aicpa-cima.com.



cloud or IoT vulnerabilities, requiring businesses to have a more adaptive, intelligence-driven approach to cybersecurity resilience”.

FINANCE-LED SOLUTIONS

Prevention

Finance can provide many remedies and mitigations in different areas. To protect valuable operations from ever-more-potent cyberthreats, companies need to be proactive, meticulous, and act with accountability. Finance can help lead in all these areas.

Kimberly Ellison-Taylor, CPA, CGMA, CEO of KET Solutions, said, “We need to be more diligent, and not just in contracts with vendors, which are in place for when it happens. We need to [be] more preventative ... so that it doesn’t happen.”

Ellison-Taylor, a former chair of the AICPA and the Association of International Certified Professional Accountants, advocates for strict compliance with existing regulations, for example around properly maintaining and

protecting data. The reputational risk of not doing so can outweigh the financial hit from losing clients, customer legal action, and paying fines.

In extreme cases, “if the criminals were able to get in and breach financial data, there could be jail time for the leaders in the organisation,” she added.

Third-party security

Because a business’s vendors and suppliers can be their weakest links, these third parties also need to have strong “cyber hygiene”. Tackling payment fraud should involve robust internal controls, which include compiling a master list of approved vendors, using bank verification tools, and requiring multiperson review, sign-off, and phone calls to approve payments and, especially, payment changes.

Finance can coordinate with IT colleagues to assess risks for their vendors and outsourced platforms. Finance can also help put contract clauses in place for meeting cybersecurity expectations. This is particularly important for companies based in different countries and with global business relationships.

Regular training

Finance can also lead regular security awareness training with colleagues, offering the chance to share stories about recent scams and breaches, and details about the emerging threats.

This should also include evaluating staff competence, simulating attacks (“red-teaming”), stress-testing defences, identifying vulnerabilities, and having code words or challenge questions for approvals internally.

Carla McCall, CPA, CGMA, the immediate past chair of the AICPA, said some business leaders “are not paying attention to the risks and [not] valuing what could stop that from happening”. They need to make sure, she added, as “there [are] repercussions from bypassing internal controls and not following the process” every time, even when staff believe something to be genuine.

TECHNICAL STEPS

This summer the UK National Crime Agency arrested four individuals in connection with

separate cyberattacks against retailers Marks & Spencer, the Co-operative, and Harrods. The nature of these breaches — including ransomware and customer data theft — and the various consequences for the companies involved (halting website ordering for six weeks, leaving shelves in their shops empty) highlights an important shift.

Businesses are having to change how they view cybersecurity. For companies, it is no longer just a technological issue but rather a business resilience problem. In other words, they need to know if the business can continue to operate if an attack takes place.

Therefore, Goldstone believes, it's fundamental that all businesses focus on the basics in protecting themselves. "That includes things like replacing older technology that's no longer getting security updates. It also means having security patching, the right configurations, strong passwords, and digital certificates to secure wireless networks and minimise the chances of someone breaching your company network. It's the basic, boring hygiene stuff — including robust backup and recovery processes — that's 90% of the battle in making and keeping your business secure."

Multifactor authorisation, having a zero-trust principle to authenticate every single time, and other multiple-step procedures to verify people when they sign in are the minimum requirements to protect a business's valuable data and assets today.

McCall set out the pivotal role finance professionals have to play in combating cyberthreats: "You have to log, create, correlate, report, and alert. You cannot defend what you cannot see. You cannot see what you do not monitor. And you cannot monitor what you do not know."

What is also key is having substantive Service Organization Control (SOC) 1 and SOC 2 reports and people who understand them. Businesses should also retain logs for a long period, as ransomware often lives in a system undetected and this data is necessary for investigating the initial breach. Going further, for larger organisations, having ethical hackers on-site and a 24/7 security operations centre capturing all events and services being logged into is key.

Businesses are having to change how they view cybersecurity. For companies, it is no longer just a technological issue but rather a business resilience problem.

EVERYONE'S RESPONSIBILITY

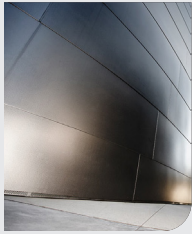
Traditionally the chief information officer (CIO), chief security officer (CSO), and chief technology officer (CTO) have been responsible for technology. However, as addressing cyberthreats has become increasingly a horizontal element essential to every function and role, it has become necessary to delegate this to every person in the business.

This means CFOs — and the wider finance organisation — of today must be equally familiar and aware of the risks as those at the executive table.

Businesses have also introduced new tools like robotic process automation (RPA) and blockchain to make processes more efficient for customers and employees. However, attackers can also hijack these systems to execute transactions and steal data and intellectual property.

To prevent criminals from being on the other side of these transactions, or at least reduce their opportunities to attack, Ellison-Taylor outlines how finance can coordinate internally. "Every single area of new technology, every single vendor partner, ERP [enterprise resource planning] system, and budget and reporting systems — you've got to make sure they're in partnership with their internal audit department."

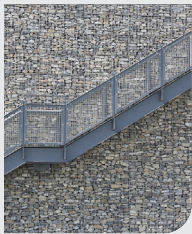
LEARNING RESOURCES



Cybersecurity Fundamentals for Finance and Accounting Professionals Certificate


This certificate programme will cover several cybersecurity topics to help you gain an understanding of the importance and impact of cybersecurity risks on your organisation or client, including an introduction to the AICPA's cybersecurity risk management reporting framework.

 COURSE



Information Security & Cyber Risk Certificate

Critical knowledge in emerging cyber and information security technologies will be gained to help you augment your accounting expertise, acquire a new skill, or complete the CITP credential.

 COURSE

What is also key is having substantive Service Organization Control (SOC) 1 and SOC 2 reports and people who understand them.

AI AS PART OF THE SOLUTION

AI is already on both sides of this equation — for the attackers and defenders, who are both seeking improvements and advantages over the other.

AI can save the game for defensive cybersecurity. Businesses can stay one step ahead by processing huge volumes of data to detect anomalies that might be a sign of a breach, such as unusual login activity or movements of data, said Rehan Qazi, FCMA, CGMA, CEO of cybersecurity business DPG-cyber.

In addition, machine-learning capabilities in tools like Tenable.io and Microsoft Defender for Endpoint can predict and prioritise potential threats, so security teams can address what matters first. “And in response to an incident, AI can save a tremendous amount of time needed to remediate a threat by correlating the alarms and suggesting remediation actions,” Qazi added.

AI-powered tools such as Darktrace, CrowdStrike Falcon, and Qualys VMDR are also patching and scanning businesses' own vulnerabilities automatically, reducing the opportunity for attack. ■

MEMBER RESOURCES

Articles

- ▶ [“How Accountants Can Combat the Rising Threat of Deepfake Fraud”](#), *FM* magazine, 19 August 2025
- ▶ [“Exploits and Cloud Complexities Test Cybersecurity Teams”](#), *FM* magazine, 8 May 2025
- ▶ [“Cyberattack Hack: The Case for Targeting Prevention Over Detection”](#), *FM* magazine, 28 March 2025

Tool

- ▶ [CGMA Cybersecurity Tool: Risk, Response, and Remediation Strategies 2025](#)