

FOR ISSUE IN THE UK AND EU  
FINANCIAL PROMOTION/MARKETING MATERIAL  
FOR PROFESSIONAL CLIENTS AND QUALIFIED INVESTORS ONLY  
NOT TO BE REPRODUCED WITHOUT PRIOR WRITTEN APPROVAL  
PLEASE REFER TO ALL RISK DISCLOSURES AT THE BACK OF THIS DOCUMENT

Insight  
INVESTMENT

# CYBERSECURITY THREATS AND TRENDS

APRIL 2025



## EXECUTIVE SUMMARY

### Matt McCormack



Matt McCormack is Managing Director and Chief Information Security Officer (CISO) for BNY Mellon, leading the Defend Platform with oversight for Cyber Security, Regulatory Engagement, Fraud Prevention, Insider Threat and Identity & Access Management. As

CISO he is responsible for defining, building, and operating a high functioning, enterprise-level cybersecurity organization that securely enables BNY Mellon's core businesses, protects the assets of the company and its clients, and preserves and enables the growth of shareholder value.

Before joining BNY Mellon in June 2022, Matt held a series of senior security executive positions, including CISO for GlaxoSmithKline Pharmaceuticals, CISO for EMC, and Global Chief Technology Officer at RSA. Throughout his career, he developed a specialized competency: designing global security operations centers for Fortune 100 companies and governments; modernizing enterprise security and risk teams; and developing cloud security migration strategies, merger-acquisition, and divestment security plans in addition to board risk management plans. He began his career as a Cryptology officer with the US Navy and spent a large part of his career working within the Federal government, assuming Senior Executive Service roles as CISO of the Defense Intelligence Agency, and Director of Security Operations at the Internal Revenue Service.

Matt maintains CISSP and CSSLP security certifications. He earned a Master of Science degree and a Bachelor of Science degree in Industrial Engineering, both from Rensselaer Polytechnic Institute and an MBA from the University of West Florida.



# INTRODUCTION

The threats posed by cybercrime to corporates and businesses are constantly evolving. As technology has become increasingly integral to both businesses and households, criminals have been incentivised to adopt ever more sophisticated techniques to exploit vulnerabilities. Consequently, businesses across the globe are projected to face costs of \$10.5trn by the end of 2025, a rise from \$3trn in 2015,<sup>1</sup>. According to Cybersecurity Ventures, during 2023 a cyber-attack occurred somewhere on earth every 39 seconds.<sup>2</sup>

Given the apparent scale of threats, we believe cybersecurity professionals are faced by three key questions:

- 1 How are cybersecurity challenges evolving?
- 2 How are viral trends influencing existing threats?
- 3 What are the potential longer-term threats to cybersecurity?

In this paper, we describe what cybercrime is, why it matters and examine each of the questions above to highlight how cybersecurity professionals are contending with the threats.

## WHAT IS CYBERCRIME

The threats posed by cybercThe International Organisation for Standardisation (ISO) defines cybercrime as “the commission of criminal acts in cyberspace”. Meanwhile, the UK government’s National Cyber Security Strategy delineates cybercrime as comprising two related, but distinct branches:

- **Cyber-dependent crimes**, which are any crimes that can only be committed using computers, computer networks or other forms of information communication technology, typically conducted via hacking and malware, including ransomware; and
- **Cyber-enabled crimes** – defined as traditional crimes facilitated by the internet and digital technologies, allowing such crimes to evolve in scale via the internet. Examples include fraud through phishing, piracy and counterfeiting.

<sup>1</sup> Cybersecurity Venture, 2016.

<sup>2</sup> Cyber security ventures, 2024.



# HOW ARE CYBERSECURITY THREATS AND DEFENCES EVOLVING?

## AN EVER LARGER AND CONSTANTLY EVOLVING THREAT

Every year, cybersecurity professionals face an ever-evolving landscape of challenges and threats, as criminals continuously innovate to outmanoeuvre existing defences. Techniques that prove effective in one domain are swiftly adapted and reapplied in another, enabling cybercriminals to partake in the staggering \$10.5 trillion cybercrime industry conducted globally each year.

The sheer scale of the estimated value lost to cybercrime underscores that what might be considered to be traditional targets, such as cash accounts and other financial assets, are not the only entities at risk. Equally concerning is the theft of intellectual property, which is crucial for innovation in a modern knowledge economy. This includes patents and scientific research. In addition, the rise in the value of cryptocurrencies has made them a significant target for theft, comparable to other financial assets. Unlike traditional currencies, cryptocurrencies can bypass global payment systems such as Euroclear or SWIFT, creating significant traceability issues for victims attempting to recover stolen funds.

Similarly, the rise of artificial intelligence and its application to media presents a formidable challenge for cybersecurity professionals. Deepfake scams, which leverage AI to create media that impersonates individuals or fabricates events, surged by 3000% in the year leading up to 2023, albeit from a low base. These scams often produce highly convincing, yet entirely fraudulent, videos of public figures endorsing bogus investment schemes, leading to substantial financial losses for victims. We delve deeper into the implications of deepfakes below. Balancing innovation with traditional defences, cybersecurity professionals are investing substantial resources to counteract novel techniques, leading to significant expenditure for businesses. Despite the application of cutting-edge technology to combat cyber-criminality, the majority of cybersecurity attacks still stem from traditional methods that exploit human error. Indeed, according to some sources, 75%<sup>3</sup> of cyber-attacks begin with an email, underscoring the importance of maintaining classic cyber techniques such as multi-factor authentication. The encouraging news for corporates is that these tried-and-true methods can be effectively applied to emerging trends within existing cybercrime techniques.

## CLASSIC TECHNIQUES CAN OFFER A SOLID FOUNDATION TO DEAL WITH EMERGING TRENDS

New technologies and criminal ingenuity have provided cybercriminals with the means to refine existing methods of exploitation, reducing the ability of potential victims to detect previously obvious scams. Fortunately, cybersecurity professionals can harness existing techniques to blunt the worst effects of these newer, more sophisticated versions of classic scams.

### Phishing and credential buying

Phishing is often regarded as the quintessential cybercrime, to the point where it has become something of a meme. Previously, phishing scams via speculative email campaigns, characterized by poor spelling and grammar, generic greetings, and incorrect email domains, were relatively easy to detect. However, the advent of artificial intelligence has made phishing scams far less obvious. Scammers can now correct grammar and spelling, adapt the email's language to a more appropriate tone, and include images that lend the scam a sense of authenticity. As a result, recipients are more likely to click on a link or enter their credentials than ever before.

<sup>3</sup> [Cybersecurity and Infrastructure Security Agency, 2022](#)



Meanwhile, credential buying represents a more insidious attempt to bypass phishing defences. This involves finding a generally low-paid employee and offering payment in untraceable cryptocurrency for the use of their username and password. Consequently, criminals can access an organisation's systems without the difficulty and time expense of hacking, effectively bypassing any anti-phishing measures.

Fortunately, existing technologies such as multifactor authentication offer a robust defence against phishing and credential buying. However, these technologies require refinements that combine digital authentication with physical confirmation of a person's identity. For example, many companies now require confirmation of identity via hardware, with a pin sent to a physical dongle to verify the identity of the person attempting to access the company's system using authorised credentials. Likewise, biometric confirmation of identity is another effective method of physical confirmation. In many respects, the need for a physical hardware component reverses the trend of security based on cloud applications and reintroduces technology from the 2000s. Organisations have realised that physical methods of security, far from being a retrograde step, offer greater control and reliability than even the most sophisticated digital solutions.

### Interview fraud

We also observe the reimposition of physical solutions to digital problems in an attempt to prevent interview fraud. Traditionally, interview fraud involved an individual conducting interviews on behalf of another in person. However, the rise of virtual interviews via video conferencing and remote working has made it easier to conduct fraudulent interviews. Deepfakes add an additional layer of deception, allowing fraudulent third parties to resemble the purported candidate

More concerningly, it is not just individuals utilising deepfakes to apply for jobs. State actors have attempted to insert operatives into large western organisations, both private and governmental, by abusing remote interviews and deepfake technology. Their goal is to gain access for their intelligence personnel and to steal finance, intellectual property or state secrets.

The mitigating action, once again, is physical. Reverting to physical interviews can potentially prevent organisations from recruiting an insider threat.

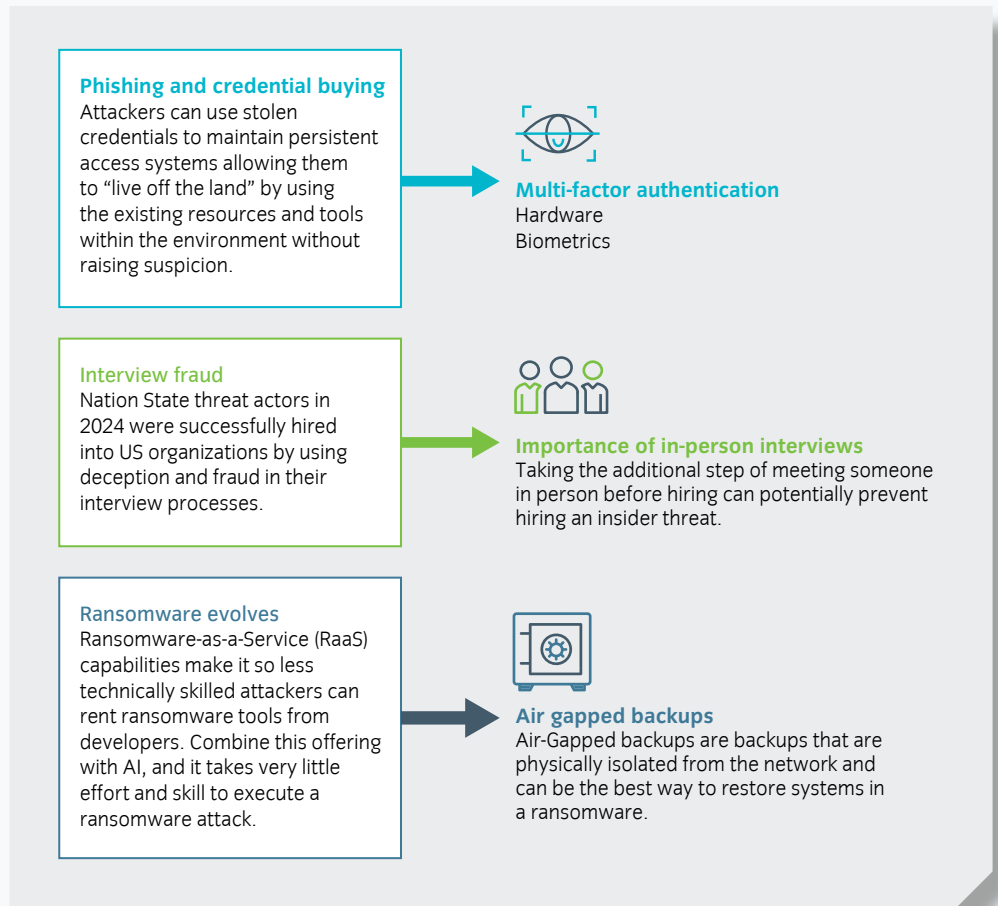
### Ransomware evolutions

Ransomware attacks, represent the most sophisticated challenge for cybersecurity professionals, due to the complexity of operations, the sophisticated nature of perpetrators and the potential costs involved in both prevention and rectification of the problem.

In simple terms, ransomware is a form of malware which encrypts a victim's data and prevents access to a computer device, with the perpetrator relinquishing control only after payment. Ransomware scams exploded during COVID, with criminals utilising professionally developed malware to target hospitals and grocery businesses.

Organisations are increasingly reverting to methods based on physical hardware to mitigate the effects of this purely digital threat. Air-gapped backups represent one potential method of preventing the worst effects of ransomware. An air gap seeks to enhance security by isolating sensitive data backups from parts of a network. While digitally based air gap solutions exist, physical air gaps may represent the most secure way of preventing ransomware attacks. A physical air gap disconnects a secure network or device by severing all wired or wireless connection, removing the ability to connect with any other network that is not within its self-contained airgap. Only those with direct physical access can interact with the data held on the air gap. While an air gap does not preclude a ransomware attack, it can be the best way to restore systems in a ransomware event.

Figure 1: Classic cyber defence techniques provide a solid foundation for emerging trends



# VIRAL CONTENT HAS MAGNIFIED THE EFFECT OF SMALL GLITCHES FOR FINANCIAL INSTITUTIONS




In addition to emerging trends, modern cybersecurity plans are grappling with the influence posed by viral content and social engineering. Viral content amplifies the effect of what would have previously been an isolated problem, heightening reputational risk, magnifying misinformation and increasing exposure to cybersecurity threats. The problem is particularly acute for consumer facing banking institutions, with several banks experiencing loss after isolated system malfunctions achieve wide dissemination via social media.

For example, in one recent instance a prominent US bank experienced a glitch relating to cheque clearance. Usually, once a cheque is deposited, the receiving bank usually mandates a specific period for the cheque to clear before the account holder can withdraw the full value of the cheque. However, due to a glitch in the bank's system, depositors could deposit a cheque and withdraw the entire value almost immediately. The bug was publicised via TikTok as a "free money glitch", which led customers to deposit worthless cheques and fraudulently withdraw funds before the cheques bounced.

While such problems have occurred in the past, social media's ability to spread information at speed can overwhelm the ability of cybersecurity professionals to identify an issue and adjust before the issue is exploited by bad actors.

Figure 2 below outlines the steps that could prevent the worst effects of viral content.

Figure 2: Navigating the risks of viral content on banking security

| Risk   | Explanation   | Steps to Prevent  |
|--|---|---|
| <br>Increased exposure to cybersecurity threats | <b>Social engineering</b> thrives on social media due to false trust, immediacy, and emotional engagement.<br><b>Viral content</b> produces excitement, curiosity, and even fear of missing out which threat actors' exploit. | <ol style="list-style-type: none"><li>1. Create a cyber response plan</li><li>2. Update social media policies</li><li>3. Employee training</li><li>4. Monitor brand presence</li></ol>          |
| <br>Heightened reputational risk                | Social media increases <b>the speed and breadth of negative information, public scrutiny and amplified criticism</b> making it harder than ever to manage reputation  | <ol style="list-style-type: none"><li>1. Create communication plan</li><li>2. Build positive presence online</li><li>3. Monitor brand presence</li></ol>  |
| <br>AI and Misinformation                       | <b>Deepfakes, manipulated images, or targeted social engineering</b> can go viral, creating major risk based on <b>misinformation</b> .   | <ol style="list-style-type: none"><li>1. Invest in AI detection tools</li><li>2. Prep rapid crisis response</li><li>3. Increase public awareness</li><li>4. Enhance security measures</li></ol> |



# FUTURE THREATS AND DETECTION

## QUANTUM COMPUTING: A DOUBLE-EDGED SWORD FOR CYBERSECURITY

---

Quantum computing is poised to revolutionise industries and existing business processes by dramatically increasing the speed at which computers process information, solving optimisation problems previously considered unsolvable. However, these capabilities also present significant challenges for businesses, particularly with regard to information security strategy.

Much of cybersecurity architecture operates based on encryption, but quantum computing could facilitate decryption of security networks previously regarded as secure. As a result, businesses and governments could face threats to apparatuses based on blockchain, experience attacks to critical infrastructure and become easily susceptible to blackmail. Given the unprecedented ability of quantum computing to break encryption, it is important for businesses to prepare for the impacts of this technology, despite it not representing an immediate threat. To mitigate these risks, we believe businesses will be best served if they:

- Stay informed of developments in quantum computing.
- Build awareness across tech security teams
- Adopt systems that can integrate with new cryptographic standards
- Monitor regulatory developments.

While these steps will not render quantum computing obsolete as a threat, they provide a solid foundation upon which businesses can develop contingencies related to quantum computing.

## DEEPPAKES: A NEW FRONTIER IN CYBERCRIME

---

Deepfake technology works by taking an existing image or video of a person and overlaying it with AI-generated content resembling an individual's voice or appearance, even allowing the generated content to mimic the person's facial movements with alarming accuracy. Deepfakes are generally used to commit fraud, disseminate misinformation, influence decisions and bypass established procedures.

While the technology is becoming increasingly complex and more difficult to detect, several signs exist that visual content is generated via AI. For videos, pay attention to facial features, the movement of which can appear slightly distorted. For audio-based content, slurring and background noise may be evident, as well as either inappropriately excessive or tempered emotional responses, depending on the context of the audio.

# CONCLUSION

The rapid pace of change within cybercrime represents a challenge for governments and businesses. Modern techniques allow cyber criminals to find new ways to exploit vulnerabilities and bypass security controls, while organisations are just beginning to feel the security considerations around AI.

While innovative countermeasures are constantly in development to mitigate the impact of cybercrime, education and awareness of new threats and trends remain critical components of any cybersecurity strategy.

## FIND OUT MORE

### Institutional Business Development

[businessdevelopment@insightinvestment.com](mailto:businessdevelopment@insightinvestment.com)

### European Business Development

[europe@insightinvestment.com](mailto:europe@insightinvestment.com)

### Consultant Relationship Management

[consultantrelations@insightinvestment.com](mailto:consultantrelations@insightinvestment.com)



[company/insight-investment](https://company/insight-investment)



[www.insightinvestment.com](https://www.insightinvestment.com)

This document is a financial promotion/marketing communication and is not investment advice.

This document is not a contractually binding document and must not be used for the purpose of an offer or solicitation in any jurisdiction or in any circumstances in which such offer or solicitation is unlawful or otherwise not permitted. This document should not be duplicated, amended or forwarded to a third party without consent from Insight Investment.

Insight does not provide tax or legal advice to its clients and all investors are strongly urged to seek professional advice regarding any potential strategy or investment.

For a full list of applicable risks, investor rights, KIID/KID risk profile, financial and non-financial investment terms and before investing, where applicable, investors should refer to the Prospectus, other offering documents, and the KIID/KID which is available in English and an official language of the jurisdictions in which the fund(s) are registered for public sale. Do not base any final investment decision on this communication alone. Please go to [www.insightinvestment.com](https://www.insightinvestment.com)

Unless otherwise stated, the source of information and any views and opinions are those of Insight Investment.

Telephone conversations may be recorded in accordance with applicable laws.

**For clients and prospects of Insight Investment Management (Global) Limited:** Issued by Insight Investment Management (Global) Limited. Registered office 160 Queen Victoria Street, London EC4V 4LA. Registered in England and Wales. Registered number 00827982. Authorised and regulated by the Financial Conduct Authority. FCA Firm reference number 119308.

**For clients and prospects of Insight Investment Management (Europe) Limited:** Issued by Insight Investment Management (Europe) Limited. Registered office Riverside Two, 43-49 Sir John Rogerson's Quay, Dublin, D02 KV60. Registered in Ireland. Registered number 581405. Insight Investment Management (Europe) Limited is regulated by the Central Bank of Ireland. CBI reference number C154503.

© 2025 Insight Investment. All rights reserved.