Insight INVESTMENT

CYBERSECURITY THREATS AND TRENDS CHECKLIST

MARCH 2025

BNY | INVESTMENTS

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.

OVERVIEW

The threats posed by cybercrime to corporates and businesses are ever evolving. The proliferation and importance of technology to businesses and households has incentivised criminals to adopt increasingly sophisticated techniques to exploit weaknesses in service to their goals.

Consequently, businesses across the globe are expected to face costs of $10.5trn by the end of 2025, a rise from $3trn in 2015[1]. According to Cybersecurity Ventures, during 2023 a cyber-attack occurred somewhere on earth every 39 seconds.[2] At the same time, there are several burgeoning threats of which businesses should be aware.

In this checklist, we delve into a comprehensive array of existing, emerging, and future threats that cybersecurity professionals must vigilantly monitor. We also present case studies that illustrate the sophisticated methods employed by cybercriminals to exploit these vulnerabilities.

[1] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[2] Cyber security ventures, 2024.

CYBERSECURITY THREATS AND PROTECTION – A CHECKLIST

PROBLEM ONE – PHISHING AND CREDENTIAL BUYING

Advancements in technology and the ingenuity of cybercriminals have enabled them to refine existing exploitation methods, making previously obvious scams harder for potential victims to detect. Fortunately, cybersecurity professionals can leverage established techniques to mitigate the impact of these more sophisticated versions of classic scams.

Phishing: An evolving cyber scam

The advent of artificial intelligence (AI) has empowered cybercriminals to create more sophisticated iterations of traditional scams. For instance, modern phishing scams are far less conspicuous than their predecessors, lacking the obvious flaws that once made them easily identifiable. AI can seamlessly correct grammar and spelling errors, while AI-generated images lend phishing emails an air of authenticity that can deceive even the most vigilant recipients.

Credential buying: Empowered by crypto

Credential buying involves targeting low-paid employees and offering them payment in untraceable cryptocurrency in exchange for their username and password. This method enables cybercriminals to infiltrate an organisation's systems effortlessly, bypassing the complexities and time-consuming efforts associated with traditional hacking techniques.

SOLUTION ONE THE POWER OF MULTI-FACTOR AUTHENTICATION

We believe that implementing multi-factor authentication (MFA) is crucial for adding an extra layer of security. The most effective solutions combine digital authentication with physical confirmation methods, such as hardware tokens and biometric verification. Many companies now require identity confirmation via hardware, using a pin sent to a physical dongle instead of a mobile phone, to verify the identity of the person attempting to access the company's system with authorized credentials. Biometric confirmation of identity is another robust method of physical verification.

CASE STUDY: Pharmaceutical company experiences credential buying

A major global pharmaceutical firm hired a software developer contractor, ostensibly based in New York City. However, according to the employee's geolocation software, they appeared to log in to the company's system while located in Pakistan, a location in which the company had no physical presence.

Upon investigation by the firm, the contracted employee appeared to work for three different companies. However, the relevant employee had subcontracted relatives in Pakistan, while receiving salaries, to complete the terms of the three employment contracts. Accordingly, to login to the company's system the contracted employee's relatives would receive the employee's RSA authorization pin via a phone call, allowing them to login.

While the firm could block the connection to Pakistan, the incident unveils an ingenious method to circumvent digitally based verification that may have succeeded had the employee's relatives been in a less conspicuous country, highlighting the potential ability to render digitally-based verification systems ineffective.

PROBLEM TWO – INTERVIEW FRAUD

We are witnessing a resurgence of physical solutions to digital problems, particularly in efforts to combat 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, which are AI-manipulated video images, add an additional layer of deception, allowing fraudulent third parties to resemble a supposed 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 exploiting remote interviews and deepfake technology. Their goal is to gain access for their intelligence personnel and to steal finance, intellectual property, or state secrets.

SOLUTION TWO PHYSICAL INTERVIEWS ARE CRITICAL

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

CASE STUDY: State actor uses deepfake to infiltrate cybersecurity company

One of the most prominent examples of interview fraud involved, ironically, a major cybersecurity firm. The company in question initiated a hiring process to hire a remote software engineer. The company conducted video interviews, and after implementing thorough hiring security protocols, such as background checks and reference verifications, the candidate was hired. However, at some, point after the candidate was hired, the company detected malware loaded onto a company workstation sent to the worker.

Accordingly, the new remote software engineer was revealed as a North Korean citizen, working for a regime linked criminal ring. The attack was deemed highly sophisticated, and the deception involved the worker using a valid identity stolen from a US-based individual and a stock image augmented by artificial intelligence, allowing the worker

The company speculated the goal of the worker was to raise funds for the North Korean regime, given the individual seemed to complete work and the relatively high remuneration the position paid.

PROBLEM THREE – RANSOMWARE

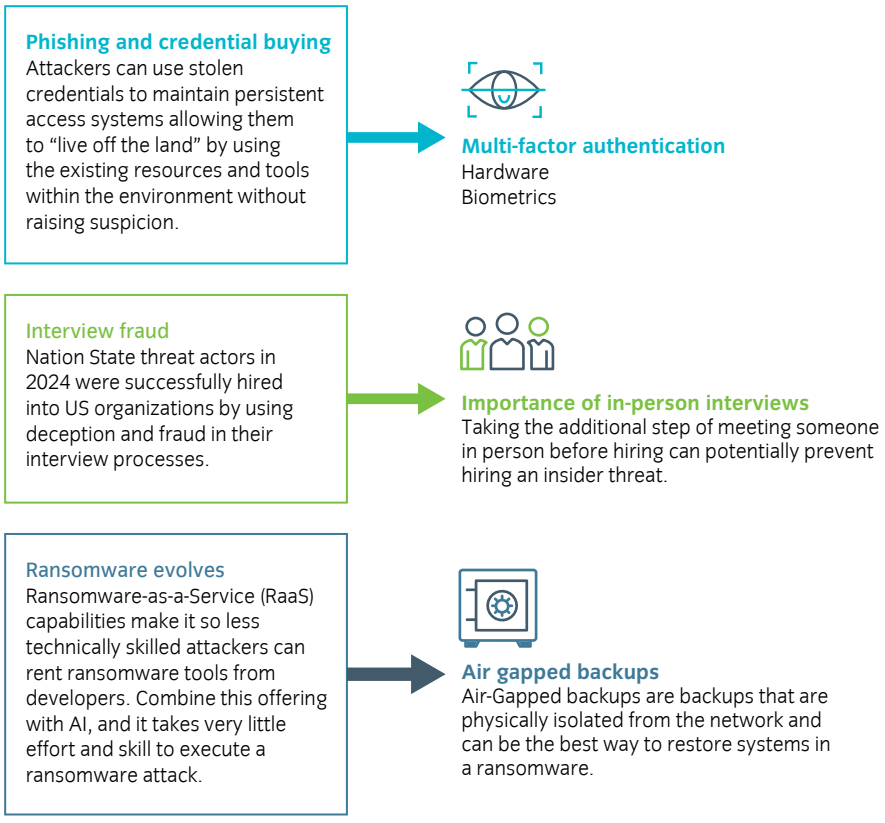
It is important to understand how ransomware is evolving and why older security protocols may offer protections

In simple terms, ransomware is a type of malware that encrypts a victim's data and blocks access to their computer device, with the perpetrator only relinquishing control after receiving payment. Ransomware scams surged during the pandemic, as criminals used professionally developed malware to target hospitals and grocery businesses. To counter this purely digital threat, organisations are increasingly reverting to physical hardware-based methods.

SOLUTION THREE AIR-GAPPED BACKUPS

These are one effective way to mitigate the worst effects of ransomware. Essentially, an air gap enhances security by isolating sensitive data backups from the network. While digital air gap solutions exist, physical air gaps are often the most secure method of preventing ransomware attacks. A physical air gap disconnects a secure network or device by severing all wired or wireless connections, preventing interaction with any other network outside its self-contained air gap. Only those with direct physical access can interact with the data held within the air gap. Although an air gap does not completely prevent ransomware attacks, it can be the best way to restore systems in the event of such an attack.

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



PROBLEM FOUR – VIRAL CONTENT AND SOCIAL ENGINEERING

Modern cybersecurity plans must address the impact of viral content and social engineering. Viral content can amplify isolated issues, increasing reputational risk, spreading misinformation, and exposing cybersecurity vulnerabilities. This problem is particularly severe for consumer-facing banking institutions, with several banks experiencing losses after isolated system malfunctions were widely disseminated via social media.

While such issues have occurred in the past, the rapid spread of information on social media can overwhelm cybersecurity professionals' ability to identify and address problems before they are exploited by malicious actors.

SOLUTION FOUR MONITOR SOCIAL MEDIA

Understand your potential vulnerabilities and be vigilant with monitoring of social media chatter related to your firm.

CASE STUDY: Major US bank suffers loss from viral storm

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.

For example, if a customer deposited $1,000, rather than waiting the enforced clearing period, the customer could withdraw the money almost immediately. The largest individual deposit and withdrawal amounted to $290,000.

A NEW FRONTIER: REMAIN COGNISANT OF FUTURE THREATS THAT YOU MAY FACE

Cybersecurity threats naturally evolve alongside technological advancements. Looking ahead, businesses should prepare for two major potential challenges: the rise of quantum computing and the continued use of deepfakes. Quantum computing has the potential to break current encryption methods, posing a significant risk to cybersecurity. Deepfakes, which are AI-manipulated video images, add an additional layer of deception, allowing fraudulent third parties to resemble a supposed candidate

PROBLEM FIVE – NEW THREATS WITH QUANTUM COMPUTING: A DOUBLE-EDGED SWORD FOR CYBERSECURITY

Quantum computing has the potential to break current encryption methods, posing a significant risk to cybersecurity. Quantum computers can process information at unprecedented speeds, potentially decrypting security networks previously regarded as secure. This could lead to attacks on critical infrastructure, blockchain-based systems, and increased susceptibility 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.

SOLUTION FIVE INTEGRATE WITH NEW STANDARDS

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 threat, they provide a solid foundation upon which businesses can develop contingencies related to quantum computing.

PROBLEM SIX – DEEPFAKES: 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.

SOLUTION SIX LOOK FOR INCONSISTENCIES

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. It is important to recognise the potential threats to your organisation and to consider how your cyber security strategy can mitigate these risks. We hope that you have found this summary useful.

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

Consultant Relationship Management
consultantrelations@insightinvestment.com

European Business Development
europe@insightinvestment.com

company/insight-investment

www.insightinvestment.com

16316-03-25