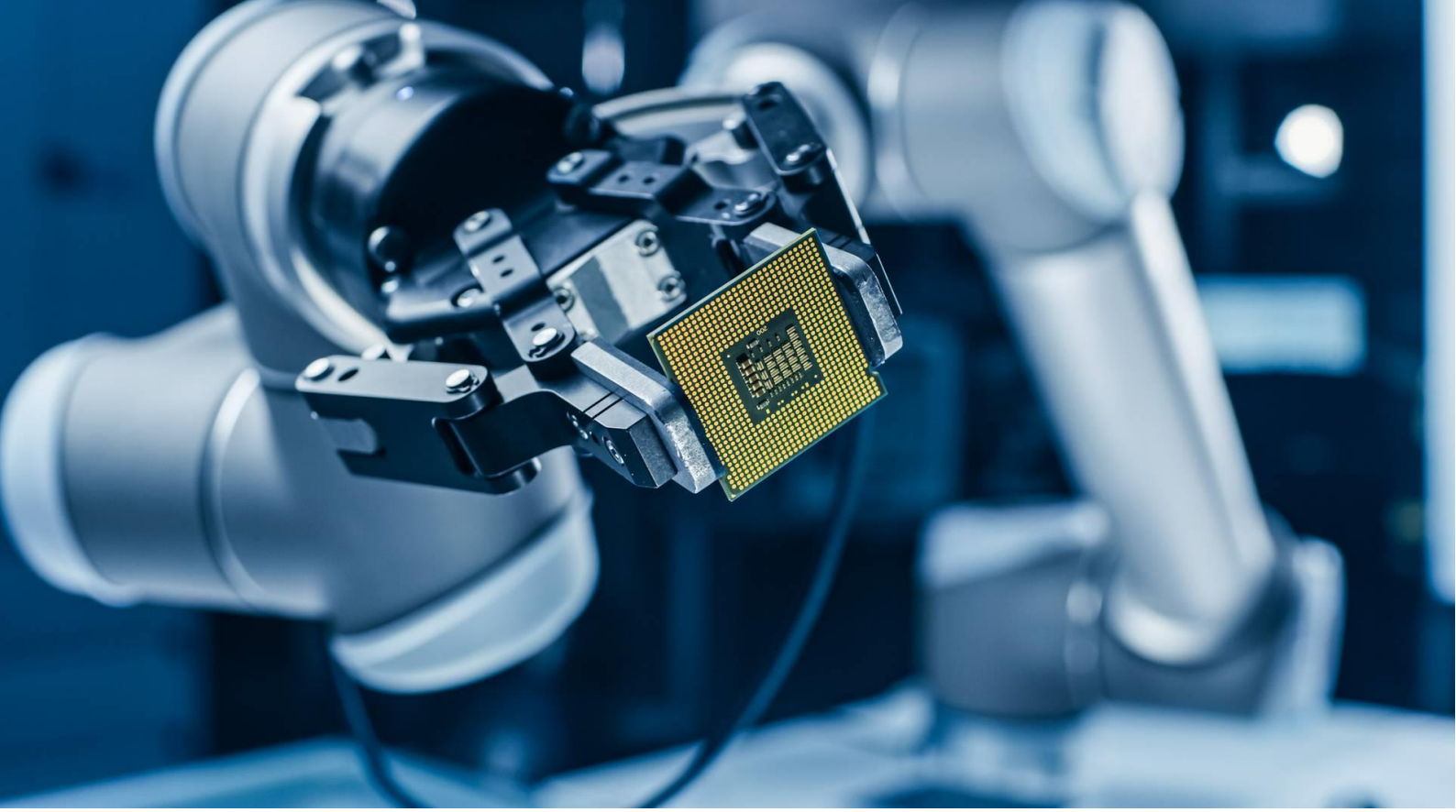

BRUNSWICK

BRUNSWICK CYBERSECURITY & DATA PRIVACY

Quarterly Cyber Trends 2025

February 2025

Introduction

In this edition of Brunswick's Quarterly Cyber Trends note, we explore how the cyber threat has evolved over the past few months.

The key takeaways for businesses are as follows:

- **Cyber threat actors continue to diversify their revenue streams**, including via insider trading and the sale of confidential information for market manipulation purposes. Crisis scenario planning should account for this possibility, recognising that threats to business are not just limited to data exfiltration and operational shutdowns.
- **Countries are increasingly going public** with the identities, means, and motives of cyber threat actors, bringing transparency to what has historically been a very opaque industry. For businesses, this means that historical cyber incidents which were not reported on at that time may generate interest months and/or years down the line.
- **The proliferation of deepfakes continues to accelerate** with threat actors developing ever more sophisticated tactics to better target companies and individuals. Crisis response strategies must therefore account for how deepfakes are transforming the threat landscape – and recognise that the tool's capacity for mass reputational damage and fraud.

If you have any questions, please reach out to the Brunswick Cyber team.

Threat actors: cyber-enabled insider trading

The view that cyber threat actors generate revenue solely through ransom payments is incorrect. Threat actors are consistently finding new ways to monetise their activities. With governments increasingly exploring new methods to reduce the flow of illicit funds to cyber threat actors – with the UK recently announcing a consultation in January 2025 to ban public sector bodies from paying ransoms – there is an incentive for threat actors to diversify.

Using stolen data to conduct insider trading is one such method, with a range of threat actors having been found guilty over the past two years. Russian criminal Vladislav Klyushin – recently freed in a US-Russia prisoner swap – had been found guilty in 2023 of engaging in a hack-and-trade scheme which saw him steal confidential data from publicly listed companies to inform his trading. In 2024, the SEC charged UK citizen Robert B. Westbrook with hacking into five publicly listed US companies to *"obtain nonpublic information about their corporate earnings and using that information to make approximately $3.75 million in illicit profits"*.

This threat, however, is not a new one – with evidence showing it has been observed in one form or another for nearly a decade. In 2015, it was reported that the US SEC was investigating a group of hackers suspected of *"breaking into corporate email accounts to steal information to trade on, such as confidential details about mergers"*. In 2017, the US Justice Department sentenced a hacker to 30 months in prison for stealing confidential company data which he then shared with traders to make insider trades.

In at least one instance, a threat actor was found to be explicitly seeking unethical traders to sell insider information to. Ransomware group DarkSide was reported to be selling intel to traders in order to encourage short-selling and the collapse of victims' stock prices. This method of monetisation poses significant reputational and business risks for companies, as it introduces both the possibility of insider-trading investigations as well as potentially enabling threat actors to directly manipulate victims' share prices for financial gain.

Threat intelligence: increasing transparency

Countries are increasingly going public with the identities, means, and motives of cyber threat actors. The UK's NCSC flagged Russian government asset Unit 29155 as being responsible for a *"campaign of malicious cyber activity targeting government and critical infrastructure organisations around the world"*, a decision which UK newspaper The Times described as *"unprecedented"*. NCSC head Richard Horne, in his maiden speech to the public, flagged a trebling of "*severe*" incidents amid Russian *"aggression and recklessness"* and China's *"highly sophisticated"* digital operations, before going on to emphasise that the risk to the UK from such actors was *"widely underestimated"* and that there was *"no room for complacency"* from UK critical infrastructure, supply chains, the public sector, and the wider economy. In addition, the UK government announced in January 2025 a consultation into proposals which would require all cyber victims to report incidents to the government – a move which authorities claim was in response to concerns that victims were keeping incidents secret and therefore potentially impacting law enforcement's ability to *"warn of emerging ransomware threats, and target their investigations"*.

The UK's NCA published in December 2024 significant details of its *"Operation Destabilise"* investigations, which exposed a multibillion-dollar money laundering scheme which enabled Russian spies and European criminals to evade sanctions using cryptocurrency. As part of the operation, the NCA provided the names, personal details, and photos of the individuals at the centre of the scheme. Separately, the NCA also published a profile of LockBit's secretive leader LockBitSupp, identifying him as Russian national Dmitry Khoroshev and even including a picture of the subject. The US's simultaneous OFAC announcement also contained his email address, date of birth, and cryptocurrency account details. LockBitSupp had previously offered a $10 million reward to anyone who could reveal his identity.

This shift towards transparency has not been limited to Western nations: the Russian government claimed in 2023 that the US's National Security Agency had compromised *"thousands of iPhones"*, including those owned by diplomats from Israel, Syria, China, and NATO members. Russia-based cybersecurity company Kaspersky Labs confirmed that *"dozens"* of employee phones were compromised in the operation – but highlighted that they *"could not comment on Moscow's allegations that Americans were responsible for the hacking or that thousands of others had been targeted*. In the same year, the Chinese government published a report claiming that the US had an *"empire of hackers"* which had been targeting *"critical information infrastructure, aerospace, research institutions, oil and petrochemical industries, large internet companies, and government agencies in various countries"* since at least 2011.

As governments provide greater detail into the activities of threat actors, there will be increased scrutiny of said activities by media and other stakeholders – which may lead to further information being released or discovered. As a result, historical incidents which otherwise may not have attracted much attention could be revisited – especially if new facts or information about the threat actor becomes public. Companies' crisis response processes must therefore account for the possibility that they may face questions about cyber incidents months or years down the line.

Deepfakes: an accelerating threat

The use of deepfakes by threat actors has continued to accelerate, with techniques becoming ever more sophisticated. Corporate executives were found to be increasingly targeted with *"hyper-personalised phishing scams generated by artificial intelligence bots"*, with industry experts noting that these AI-generated attacks are more likely to *"bypass companies' email filters and cyber security training"*.

Using deepfakes of corporate leaders to commit fraud has already seen some success. A successful deepfake attack cost engineering group Arup $25 million, with the threat actor using a digitally cloned CFO to trick staff in Hong Kong into transferring money into threat actor-controlled accounts. A failed attempt to use a deepfake of Ferrari CEO Benedetto Vigna was thwarted when the targeted senior executive – who the threat actors were attempting to convince to authorize a transaction – requested verification that he was in fact speaking to Vigna. Another failed attempt at a different company saw a deepfake of WPP CEO Mark Read being used to target a senior WPP leader in order to solicit money and personal details.

Corporate leaders are not the only potential targets. An investigation by the Hong Kong Police led to the interception of over USD 3.37 million in scam proceeds, much of which had been stolen by a criminal syndicate which used AI to generate *"credible images of attractive women to lure victims into romance and investment scams"*. A recent BBC investigation discovered that audio deepfakes were able to beat bank security checks – hypothetically giving threat actors access to their targets' bank accounts. Finally, an uptick in threat actors using deepfakes of celebrity doctors to promote "*cures*" for serious health problems has been observed – with some of the alleged cures being dangerous to human health.

As deepfakes continue to proliferate, companies must ensure that their crisis response plans include a dedicated deepfake plan. Responding to a deepfake incident is fundamentally different to other types of crises. The falsification of evidence combined with tailored and aggressive targeting of key stakeholders means that the situation can escalate quickly – leaving targeted businesses with little time to plan and respond. In addition, it may be difficult to provide conclusive proof that the content is false – requiring companies to rely on stakeholders giving them the benefit of the doubt in the initial stages of an incident. The potential financial and reputational risks of a successful deepfake attack are therefore significant and require specialised response strategies and resilience training.

To continue the conversation, contact our team:

Nicola Hudson

Partner, Cybersecurity, Data & Privacy Global Lead, London

nhudson@brunswickgroup.com

Nicola has worked on hundreds of cybersecurity incidents and has deep expertise in cybersecurity issues and crisis management across both the public and private sector. Prior to joining Brunswick, she was a member of the Executive Board at GCHQ and Director of Policy at the National Cyber Security Centre, joining the centre as one of the founding Directors in 2016.

Paddy McGuiness

Senior Advisor, London

pmcguiness@brunswickgroup.com

Paddy supports clients on crisis and resilience and the interplay between geopolitics, national security and their transactions. From 2014 to 2018, Paddy was the UK's Deputy National Security Advisor for Intelligence, Security and Resilience, advising two successive British Prime Ministers on UK Homeland Security policy, capabilities and related legislation.

Suntka von Halen

Partner, Munich

svonhalen@brunswickgroup.com

Suntka specializes in restructuring, crisis and cybersecurity, change communications and corporate positioning. As Co-Lead of Cybersecurity Germany, she supports clients in crisis preparedness and within Brunswick's global cyber crisis team works on many cross-border crisis response mandates. Prior to joining Brunswick, she worked in the media industry for more than 10 years and served as spokesperson at Gruner + Jahr (a Bertelsmann company).

Marina Bidoli

Partner, Milan

mbidoli@brunswickgroup.com

Marina is a senior client advisor on business-critical issues. Her stewardship has included four-and-a-half years as Head of Brunswick South Africa, where she led South Africa's cyber and crisis practice groups. Prior to joining Brunswick, Marina headed Group Communication at Sasol, the JSE-listed integrated energy and chemicals group.