CYBERSECURITY, DATA & PRIVACY

Cyber Trends – Spring 2024

Introduction

Welcome to the first edition of the relaunched Brunswick quarterly cyber trends note. Each quarter we will explore several cyber and cyber-adjacent topics which businesses should be thinking about. The key takeaways for businesses are as follows:

- **Both state and nonstate actors have integrated artificial intelligence (AI) into their offensive operations, making phishing attacks increasingly plausible. Sensitising staff to these new forms of socially engineered attacks is ever more important.**
- **Ransomware actors are spending at scale – including offering bribes to employees of target companies – to improve the likelihood of a successful intrusion. Management of insider risk, including down supply chains, is too often neglected when ensuring cybersecurity.**
- **Companies may be targeted as part of a wider attempt to disrupt and/or weaken public trust in government and societal institutions. A tailored response with specific expertise and knowledge of both state threats and the intelligence agencies is needed.**
- **The cyber-capabilities gap represents a growing threat for companies with global operations. Prepare for significant variations in response across jurisdictions even within regulatory blocs such as the EU, US, India or China.**

AI: the impact on the cyber threat

AI's effect on cyber defence and offense is still in its early stages, but it will be transformative. Actors on both sides are likely to see a significant capability uplift with potential greater advantage for defence. For companies, AI's most immediate impact is as Shadow IT – where employees use AI applications for work without company oversight or, in the worst case, awareness.

Both state and nonstate threat actors have begun integrating AI across their offensive operations. Key use cases include more sophisticated social engineering within phishing attacks, the enhancement of reconnaissance techniques, and the semi-automation of malware development and mutation. From a defensive standpoint, the greatest uplift has been in the application layer where quality and consistency as well as efficiency are being transformed. Companies are rolling out technologies that utilise ever faster behavior-based analytics to detect abnormal activity within a network, automated threat intelligence which allows real-time updates on the threat landscape and the integration of AI into incident response training.

Whilst AI's impact on cybersecurity is likely to be significant, it is important to take a considered, longer-term view rather than obsess about a single technology. Ensuring that companies have the practiced capability and capacity to respond to and recover from cyber incidents remains the keystone to protect value and reduce or avoid business interruption.

Ransomware: spending money to make money

Over the past five years, the ransomware industry has grown exponentially despite increasing cross-border law enforcement. Chainalysis estimated that total ransomware payments exceeded $1 billion in 2023, a near five-fold increase from the estimated $220 million paid in 2019. There is therefore a strong incentive for ransomware actors to invest money into maximising the likelihood of a successful attack.

The 'zero-day vulnerability market' refers to the buying and selling of previously unknown security flaws. Major technology corporations such as Apple have established bug bounty payouts, which pay between $5,000 to $2 million. Third-party exploit sellers, which sell exploits to corporate and government clients, may offer higher sums – Zerodium is offering up to $2.5 million. Criminals, however, are willing to offer significantly more – with a report in 2021 recording offers of up to $10 million from dark-web threat actors.

People continue to be the biggest cybersecurity threat to organisations. Whilst the industry's focus has primarily been on human error, this risk also includes malicious employee activity. A survey of 100 IT and security executives found that 65% of companies had found that their employees had been approached to assist in ransomware attacks – with ~40% of these employees being offered at least half a million US dollars – in either cash or bitcoins – for their support.

The significant financial reward of ransomware – and of selective IP theft – incentivises threat actors to offer monetary rewards to insiders. A key indicator of resilience in an enterprise is the interplay between the people, security and cyber functions with a clear definition of roles, modelling of plausible risks and exercising against them. Care is needed in management and communication of such work to create the right level of curiosity in the workforce whilst avoiding excessive distrust.

Geopolitics: the cyber threat to public trust

With increasing geopolitical tensions worldwide, state actors seeking a low-cost and low-risk method of promoting their interests can launch cyberattacks on nongovernmental entities to indirectly weaken public trust in government and societal institutions. In 2022, a group of local residents who lived near a hospital that had been hit by ransomware were surveyed on the incident. The results found that the residents' trust in the government and security agencies had fallen because of the attack. Recently, the Canadian Communications Security Establishment warned that Russia-aligned nonstate threat actors were likely aiming to compromise Canada's oil and gas sector in order to generate a 'psychological impact' amongst Canadians to 'weaken Canadian support for Ukraine'.

As geopolitical tensions ramp up and many states make use of cyber and disinformation tools below the threshold for an act of war, the likelihood of companies being impacted – whether directly or indirectly – increases. Election periods represent an opportunity for state threat actors to maximise their destabilising impact on political processes. Companies should therefore ensure resilience and response protocols are current and include tailored provisions and strategies in the event a state-aligned threat actor launches an attack.

Food for thought: the cybersecurity equity gap

The cybersecurity equity gap refers to the growing divide between the most- and least-resourced entities across the globe. This cybersecurity gap, which exists in both the public and private sectors, represents an alarming risk for all stakeholders due to the interconnected nature of the global cyber ecosystem. Companies with international operations and subsidiaries may therefore be unknowingly exposed to cyber risk due to weaker cybersecurity capabilities in some markets.

Historical research into this equity gap has found that it benefits threat actors, who can leverage the globalised nature of supply chains to target the most insecure link in the chain to reach their victims. One report estimated that there had been a 200% increase in open-source supply chain attacks in 2023 compared with 2022. Another report found that 98% of organisations have a relationship with at least one third party that has experienced a breach in the last two years.

This capabilities gap is not limited to companies; similar divides exist between governments, with consequences for global cooperation and international relations. It was reported that the US government had been hesitant about sharing defence-related information with Japan due to concerns around cybersecurity standards. The Philippine government acknowledged that its inability to provide competitive pay for cybersecurity experts meant that it was, in some instances, forced to work with “black hat” hackers who may have attacked government websites. The capabilities and roles of cybersecurity centres and regulators varies enormously between jurisdictions even within regulatory blocs such as the EU.

The cybersecurity equity gap remains a difficult challenge to address, with major consequences for the cyber ecosystem. Companies need to regularly update their cybersecurity resilience plans and strategies – as well as their exposure to third-parties across their entire global footprint. Companies with global footprints should be aware of the uneven cybersecurity capabilities across their markets and ensure they are accounted for when building resilience and crisis management plans.

Senior Leadership

Paddy McGuinness

Senior Advisor, London

Email

+44 207 404 5959

Paddy is a Senior Advisor at Brunswick Group, supporting clients on crisis and resilience and the interplay between geopolitics, national security and their transactions. He works closely with the firm's regional and specialist leads across Technology, Cyber, Litigation, Geopolitical, Activism and Competition and Regulatory Affairs. 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.

Yasmin Brooks

Partner, Cybersecurity, Data & Privacy Global Lead, London

Email

+44 207 404 5959

Yasmin specializes in crisis response, resilience and data privacy. She supports clients across multiple sectors and geographies as they navigate a range of cyber risks. Yasmin spent nearly two decades in UK Government where she led on a number of cyber issues, including a national cyber strategy, the formation of the National Cyber Security Centre and a range of data and cyber legislation.

Nicola Hudson

Partner, Cybersecurity, Data & Privacy Global Lead, London

Email

+44 20 7404 5959

Nicola joined Brunswick as a Partner in the cyber practice in 2022. She has worked on hundreds of cyber security 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, having joined the centre as one of the founding Directors in 2016.

Suntka von Halen

Partner, Munich

Email

+49 151 1688 2769

Suntka specializes in restructuring, crisis and cybersecurity, change communications and corporate positioning. As Co-Lead 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 in 2016 she worked in the media industry for more than 10 years and served as spokesperson at Gruner + Jahr (a Bertelsmann company)..

Senior Leadership

Alexandra Abreu Loureiro

Partner, Lisbon

Email

+44 788 959 1836

Alexandra heads Brunswick's senior advisory in Portugal and the Portuguese-speaking world. She specializes in crisis situations, having advised a number of international clients in Portuguese-speaking territories. Prior to Brunswick, Alexandra was an award winning broadcaster on Portuguese television, served in the Portuguese Government as Head of Communications and spokesperson for the Ministry of Defence of Portugal and special advisor for the State Secretary of Foreign Affairs and Development Aid.

Marina Bidoli

Partner, Milan

Email

+39 342 3685318

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.

EMEA Cybersecurity, Data & Privacy Team

Nick Roodman

Director, Johannesburg

Nick is a core member of Brunswick Johannesburg's Cybersecurity team, leading cyber crisis response and preparedness mandates. He has advised companies during several of South Africa's major cyber breaches. He obtained his BCom (Law) degree from the University of Stellenbosch.

Thomas Baur

Director, Paris

Thomas is a Director in Brunswick's Paris office. With fifteen years experience in corporate communications, he advises clients on a wide range of issues including cybersecurity, campaigns, media relations, digital strategies, and crisis management. Prior to joining Brunswick in 2022, he worked in the communications departments of VINCI, EY, and Keolis

Elisa Lavagna

Director, Milan

Elisa is a Director at the Milan Office and specialises in corporate positioning, litigation, restructuring and crisis communications. She is a member of Brunswick's European Cybersecurity Group, helping organizations respond to cyber issues. Prior to joining Brunswick in 2014, Elisa worked for leading PR agencies in Italy.

Cecilie Oerting

Associate, London

Cecilie spent six years with Brunswick in Singapore and recently relocated to London. She specializes in crisis management and corporate positioning, with a specific focus on cybersecurity and data privacy. Prior to Brunswick, Cecilie worked on public safety and security projects at NEC Corporation and INTERPOL.

Louis Yau

Associate, Cybersecurity, Data & Privacy Practice Manager, London

Louis is an Associate in Brunswick's London office and is a member of the firm's Cyber team. He joined Brunswick in 2019 and has supported clients on a broad range of issues including navigating geopolitical tensions, crisis response and preparation, cybersecurity, global reputation and financial situations.

Charlie May

Associate, Dubai

Charlie is an Associate based in Brunswick's Dubai office, where he advises clients in the Gulf on a range of crisis and cybersecurity issues. His work includes developing incident response strategies to preserve corporate reputation during live cyber crises, as well as reputational risk mitigation through crisis preparedness work with c-suites and communications and information security teams.