nccgroup

People powered tech-enabled cyber security

Cyber Threat Intelligence

Review of October 2024

FOX IT

part of nccgroup

Executive Summary

This October, we continue to provide you with insights from the cyber threat landscape. The figures from our ransomware database suggest a 19% increase in ransomware activity, with RansomHub remaining the leading threat actor and Industrials the most targeted sector.

Away from the statistics, our ransomware spotlight discusses the recent attack on the electronics giant Casio by the Underground ransomware group, and their potential links to the Russian state. As ever, it appears that ransomware remains a prominent threat to cyber security, with the potential blurring of lines between organised crime groups and nation-states.

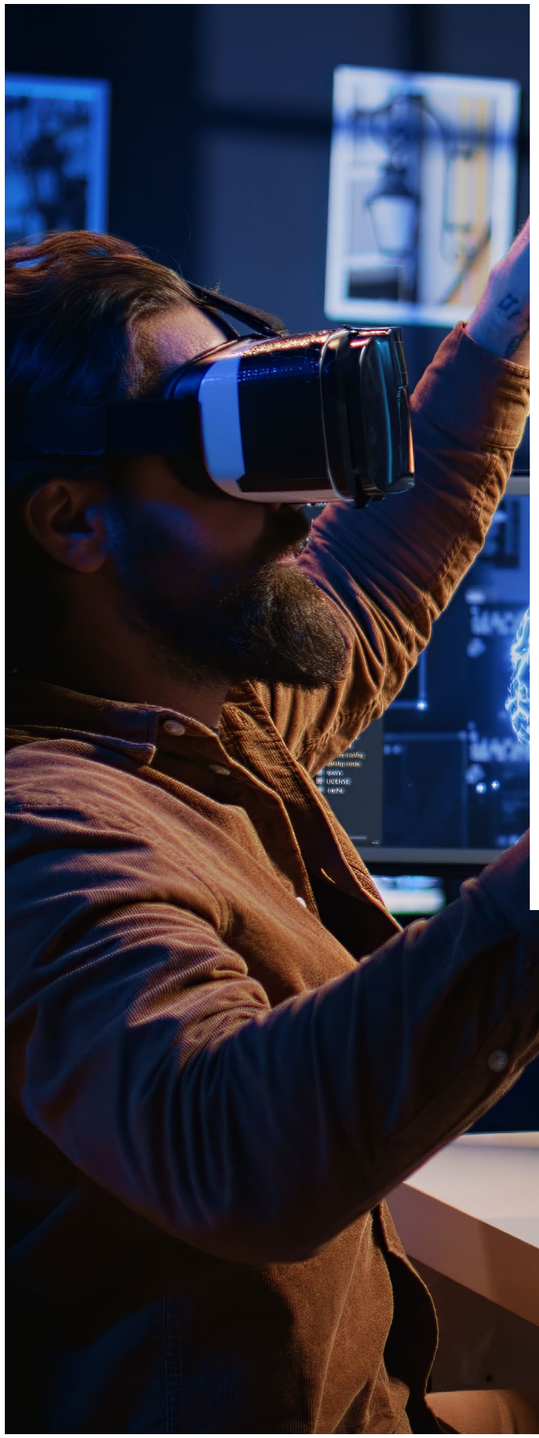
October represents the beginning of a new theme for our Quarterly Thematic Outputs, and this time we are focusing on nation-state activity. Flagged as part of the current and emerging threats by Microsoft in the recent Microsoft Digital Defense Report 2024, alongside the activity we have observed from Russia and China in line with the US elections and other geopolitical events, over the next three months, we will explore nation-state threats.

This month we introduce the topic and provide coverage of recent Russian and Chinese activity. Building on the theme of geopolitics, our Emerging Cyber Security Trend focuses on the current tensions between China and Taiwan, and how this looks from a cybercrime perspective.

The following reviews the intricacies of the dispute between China and Taiwan at present, analysing the geopolitical chessboard and the invisible battleground of cyber operations.

Equally, it considers the role of the international community in calling for dialogue and peace, while at the same time enhancing efforts to boost cyber security and minimise attacks in the region.

Overall, the threat landscape remains dynamic, with nation-states and organised crime groups moving towards greater collaboration. Mitigating attacks therefore requires continued persistent and creative efforts on the part of organisations, notably where different threat actors may benefit from each other's resources.



Contents

Section 1

Ransomware Key Statistics

19%

Global ransomware attacks increased by 19% in October

30%

Industrials accounted for 30% of ransomware attacks in October

14%

RansomHub was responsible for 14% of attacks in October

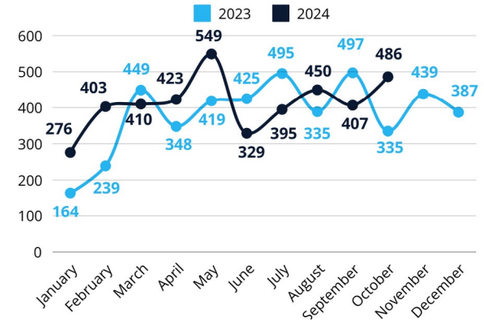


Figure 1 Number of Ransomware Attacks by Month

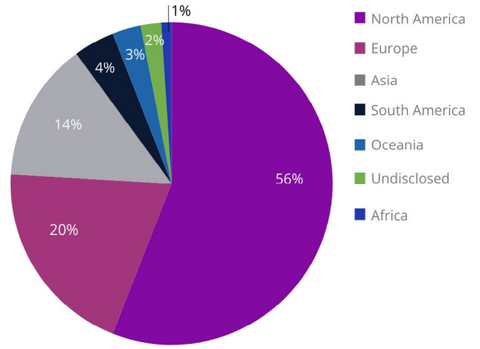


Figure 2 Ransomware Attacks by Region, October 2024

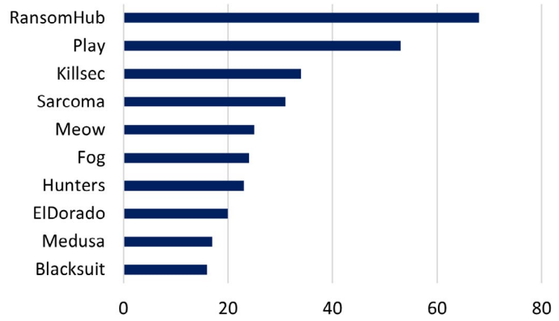


Figure 3 Top 10 Threat Actors October 2024

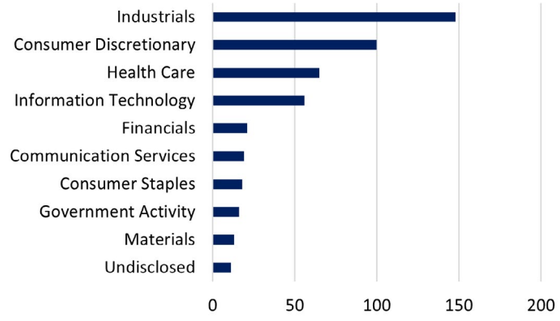


Figure 4 Top 10 Targeted Sectors October 2024

Key Events

01/10/24
UMC Health System

A ransomware attack on UMC Health disrupted IT systems, forcing the hospital to divert patients to other facilities.

16/10/24
Globe Life

The largest US provider of life and health insurance was targeted by an unknown threat actor. Stolen customer data includes names, email addresses, phone numbers, postal addresses, Social Security Numbers, health-related data, and policy information.

24/10/24
UnitedHealth

BlackCat targeted UnitedHealth resulting in the data theft of over 100 million people. The breach was traced back to a vulnerability with Citrix remote access software which hackers exploited to gain access to the system. This caused a financial impact estimated between $2.3 - $2.5 billion.

North Korean Hackers Collaborate with Play Ransomware

North Korea's Jumpy Pisces group collaborated with Play ransomware gang in a notable cyberattack, marking the first instance of a North Korean state-backed group engaging in a ransomware campaign. They gained access via a compromised user account and used tools like Sliver for lateral movement, DTrack malware for spreading, and customised Mimikatz for privilege escalation. They also uninstalled EDR sensors and deployed a trojanised binary to steal browser data.

NCC Group Services

NCC Group can support you to mitigate against the ransomware threat. Please see our contact details at the end of this report should you require assistance.

Section 2

Ransomware Spotlight:

Casio Ransomware Attack by Underground

The Casio ransomware attack in October 2024 demonstrates the ongoing threat of cybercrime against major corporations.

This research examines the breach, its broader implications, and the strategic measures organisations can adopt to enhance their cyber security defence. Ransomware groups like Underground, responsible for the Casio attack, have become adept at exploiting vulnerabilities, targeting companies that handle high-value data across interconnected networks.

The following explores why enterprises like Casio may be targeted, possible connections to the Russian State, and the potential blurring of lines between organised crime groups and nation-states.

Casio Ransomware Breach: The Attack

On October 8, 2024, the electronics giant Casio confirmed a ransomware attack that led to unauthorised data access and data theft.
The breach was initially detected when the Underground ransomware group claimed responsibility and began leaking the stolen data.

The breach primarily targeted personal information, including the details of Casio's employees, job candidates, and business partners. The company confirmed that no credit card information was compromised, and essential service systems like CASIO ID were unaffected.

However, the attack did disrupt some systems leading to service outages. The group applied double-extortion tactics, in which data is encrypted and simultaneously extracted, demanding victims to pay a ransom fee to recover data and prevent public leaks.

This double-extortion tactic has become increasingly common across the threat landscape, as it maximises pressure on companies to comply with ransom demands quickly. At present, it is unknown how the group accessed Casio's systems.

While the exact entry points of the attack have not been disclosed, it is possible that Underground exploited vulnerabilities within Casio's network.

Recent reports suggest that the Underground ransomware group has been exploiting vulnerabilities, such as the CVE-2023-36884 flaw in Microsoft Office. This Remote Code Execution (RCE) vulnerability allows attackers to gain initial access to target machines, potentially by sending malicious Office documents.

It is unknown if Underground exploited this CVE to breach Casio, however, the group's use of CVEs, even historic, emphasises the need for timely patch management as ransomware actors continue to exploit vulnerabilities. For businesses across all sectors, ensuring that systems are regularly updated and patched can prevent exploitation of known vulnerabilities.

Two weeks after the attack, Casio was still struggling to restore its systems. According to Casio's spokesperson, Ayuko Hara, several servers remained unusable, and measures taken to disconnect them have caused further disruptions.

These actions, aimed at preventing the spread of damage, have affected Casio's ability to receive and place orders with suppliers, as well as disrupted product shipments. The issue appears to primarily impact customers in Japan, who faced delays and uncertainties with shipping schedules.

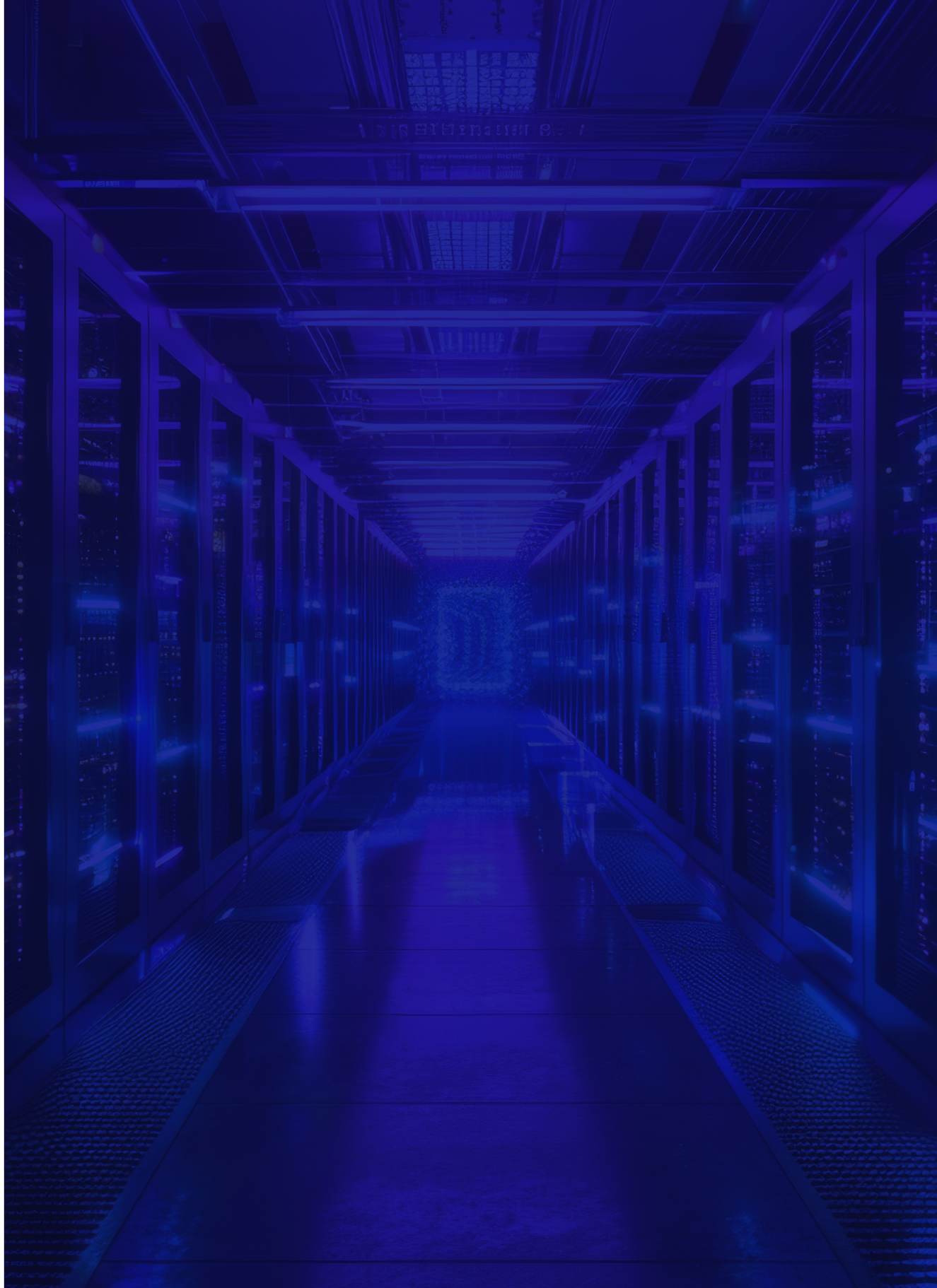
However, Casio's US website has not been affected, indicating that the disruptions are localised. This extended period of disruption however highlights the long-term consequences that ransomware can have on business operations.

Additionally, Russia's recent protests over Japan-US military drills near Hokkaido demonstrate its unease with Japan's strategic alliances. Moscow's concern over military cooperation and Japan's expanding role in regional security could have been a trigger for increased cyber aggression.

Attacks on Japanese companies could serve as a form of pressure or retaliation, signalling Russia's discontent with Japan's defence strategies. By targeting key Japanese enterprises, Russia, through affiliated cybercriminal groups, might aim to disrupt economic stability and project power without overt military confrontation.

The situation shows the complexity of modern cyber warfare, where criminal enterprises and state-backed actors could pursue both financial and strategic objectives.

The Casio incident demonstrates the possible blurring of the lines between crime groups and the domains in which they operate. As such, businesses should encompass a variety of threats, traditional and state-backed, in their defence strategy.



Section 3

Quarterly Thematic Output: Nation-States, Recent Activity and Trends

This quarter we will examine nation-state activity by delving deeper into their unique capabilities and motivations, notable attacks recorded, tools and campaigns used, as well as how these actors could influence global events around the world, for example, the US elections.

In this monthly piece, we investigate the influence Russian-sponsored adversaries had on the upcoming US elections in September and October, which would also serve as a continuation of our research so far on Misinformation, Disinformation and Malinformation. A brief overview of the latest activity conducted by Chinese threat groups, specifically focusing on influence operations, has also been included.

Nation-states – Overview of Capability and Motivations

A nation-state or state sponsored threat actor refers to a group which engages in malicious cyber activities that are either sponsored or directed by a government.

Nation-state sponsored threat groups are also known as Advanced Persistent Threats (APTs), as they are highly sophisticated and therefore considered to be the most capable and the most resourceful of all threat actor types.

These cyber adversaries tend to be driven by long-term objectives, usually linked to their wide variety of political and economic motivations. Some of the key characteristics observed across nation-state actors includes:

- **Government Sponsorship:** funded, supported, and directed by a national government.
- **Advanced Capabilities:** advanced technical skills and tools, typically surpassing those of other cybercriminals, for example, hacktivists or organised crime groups (OCGs).
- **Strategic Objectives:** aligned with the strategic interests of their sponsor, which could include espionage, disruption, destruction, or influence operations.
- **Target Selection:** including but not limited to critical infrastructure providers, governments, defence suppliers, or political entities.
- **Long-Term Operations:** a typical campaign could last for months or even years, to gather intelligence for the sponsor and to disrupt the target's operations, or even influence public opinion.

It is important to remember that this type of threat actor has a wide range of tools and techniques at their disposal to successfully achieve their long-term objectives, including:

- **Spear-Phishing:** a highly targeted type of phishing attack which is designed to trick specific individuals to either reveal or provide access to sensitive information and could also include installing malware.
- **Zero-Day:** refers to the exploitation of previously unknown vulnerabilities in software or hardware before the developers/ vendors can issue patches.
- **Advanced Malware:** a custom-built malware which is specifically designed to evade detection and perform specific tasks, such as data exfiltration or system disruption.
- **Watering Hole Attacks:** includes the compromise of websites which are frequently visited by the target to deliver malware successfully.
- **Social Engineering:** the act of tricking individuals to divulge highly confidential information via deception and psychological manipulation techniques.

Overall, nation-states engage in long-term malicious activity, which focuses on system and service disruption, data theft, and espionage.

The impact of a state sponsored attack could be extremely damaging, not only to the targeted institution or sector, but to the wider economy.

Nation-state actors may target a particular sector for multiple reasons. For example, a nation-state targeting the Industrials' sector could be particularly interested in the key role the sector plays in the global economy such as being responsible for the production of essential goods and services, which include machinery and equipment, and repair and maintenance services.

Any disruption to the typical production cycle due to nation-state activity could have devastating consequences at a global scale, which includes but is not limited to, direct financial losses, production delays, equipment damage, and in some cases, impact on human safety.

Section 4

Emerging Cyber Security Trend: The China-Taiwan Dispute: Geopolitical Challenges and Cyber Warfare Dynamics

The China-Taiwan dispute has been ongoing since 1949. The following reviews the intricacies of the dispute between China and Taiwan at present, analysing the geopolitical chessboard and the invisible battleground of cyber operations.

We discuss China's aggressive tactics of economic coercion, diplomatic isolation, and military drills to compel reunification, as well as Taiwan's cyber defences against the relentless cyberattacks.

The stakes are high. Any misstep or miscalculation could potentially escalate the situation, leading to significant regional and global consequences.

Geopolitical Tensions in the China-Taiwan Dispute

The People's Republic of China (PRC) has been increasing its assertiveness towards Taiwan leading to geopolitical tensions. China and Taiwan have been in dispute since the Chinese Civil War in 1949, when Taiwan split from Mainland China, however a recent escalation was triggered by Taiwan President Lai Ching-te's National Day speech, and subsequent Chinese military exercises around Taiwan on October 14, 2024, dubbed Joint Sword 2024B.

China's efforts, such as economic coercion, diplomatic attacks, and military threats are used to pressure Taiwan to accept their jurisdiction of the region. The PRC's reunification with Taiwan is a core view for its rejuvenation project.

However, Taiwan's democracy has refused these overtures and continues to assert its sovereignty and democratic values. The ongoing tension between the two countries has broader implications for regional stability and global security.

The potential conflict with the Taiwan Strait and West Philippine Sea could have far-reaching consequences that can disrupt global supply chains, trigger a broader regional conflict, and potentially escalate into a global confrontation.

The aggressiveness of the PRC has affected the relationship between Taiwan and other countries, Czechia for example was urged by the PRC not to interact with Taiwan, which was labelled by PRC as separatist forces.

Additionally, joint naval drills between Russia and the PRC in the Pacific highlights the strategic alliances that Beijing is growing its regional influence.

Furthermore, the PRC is considering measures in retaliation for the Taiwanese trade restriction against the PRC. As the geopolitical tension between China and Taiwan continues to escalate, it is crucial to monitor the evolving strategies of both countries.

The full versions of our spotlight, quarterly thematic output, and emerging cyber security trend research can be viewed in our Premium Threat Pulse.

This is available to Managed Service clients and those that purchase our Intelligence Subscription Service.

If you are interested in key insights and explorations on the current threat and geopolitical landscape, look no further than our research insights. These will provide you with an in-depth view of pertinent topics from AI, emerging threat actors, nation-state activity, and more.

Sign up here

About us

NCC Group is a global cyber and software resilience business, operating across multiple sectors, geogra-phies and technologies.

As society's dependence on the connected environment and associated technologies increases, we use our global expertise to enable organisations to assess, develop and manage their cyber resilience posture to confidently take advantage of the opportunities that sustain their business growth.

With circa 2,400 colleagues, we have a significant market presence in the UK, Europe and North America, and a growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

+44 (0)161 209 5200
reponse@nccgroup.com
www.nccgroup.com

People powered tech-enabled cyber security

FOX IT
part of nccgroup