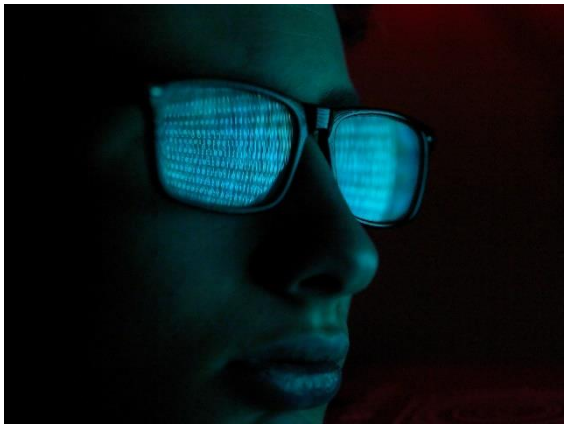
KCS Group Europe

The need for proactive investment in Cyber Security

May 2023



In March 2023, Capita, a consulting digital services business, was hit by a cybersecurity breach. Compromised data from the organisation, which works with business and government, reportedly included individuals' home addresses and passport images. Hackers were able to gain unauthorised access to Capita's internal systems using a ransomware breach, through which less than 0.1% of the server data was extracted. Significant expenses directly associated with the breach are expected, estimated to be around £15m to £20m.

The need for proactive investment in cyber security

This incident highlights the importance of proactive investment in cyber security, in order to avoid the long-term costs of such an attack. Organisations need to allocate resources for robust cyber security measures. These include regular security assessments, implementation of advanced threat detection systems, employee training on security best practices, maintaining up-to-date software and system patches, as well as establishing incident response plans. By investing in proactive security measures, organisations can reduce the risk of cyber-attacks, minimize the impact of any successful attacks, and protect sensitive data and critical systems.

Given Capita's size as an organisation, how significant are these costs?

Capita is a large organisation that provides IT outsourcing services to the government, handles sensitive data for the BBC, works on nuclear projects, and manages IT systems for councils and the NHS. Given the scale and complexity of their operations, the costs incurred by the cyber-attack are still very significant.

The potential financial impact reaches beyond immediate direct costs and includes potential reputational damage, legal consequences and regulatory scrutiny.

What are the recovery and remediation costs for organisations?

Recovery and remediation costs can be huge. Capita have allegedly paid the ransomware fee towards the Russian hacker group, 'the Black Basta gang'. Other costs will include specialist professional fees, recovery and remediation expenses, along with investment to strengthen their cyber security environment.

What needs to be done to protect one's business from cyber-attacks in the future?

To defend against cyber-attacks, several measures can be taken:

- Robust security measures: companies should invest in strong security protocols, including encryption of sensitive data, multi-factor authentication and regular security audits and assessments.
- Employee training and awareness: education of employees about the risks of cyber-attacks, phishing attempts and the importance of following security best practices is vital. This can help prevent successful attacks that exploit human error.
- Regular vulnerability assessments: companies should conduct regular assessments of their IT infrastructure to identify potential weaknesses or vulnerabilities that could be exploited by attackers.
- Incident response planning: develop a comprehensive incident response plan that outlines the steps to be taken in the event of a cyber-attack. This should include procedures for rapidly identifying and mitigating attacks, notifying affected parties and restoring systems and data.
- Collaboration and information sharing: engage in information sharing and collaboration with other industry organisations, and cyber security experts to stay updated on emerging threats and best practices for protection.

Why does it seem there are so many more cyber-attacks of late?

Several factors contribute to the increase in recent cyber-attacks, including:

- The war between Russia and Ukraine: NATO countries have been targeted by Russian threat actors more frequently since the war began.

Big organisations including Royal Mail have already been a victim to recent cyber-attacks and this is only the beginning.

- Expanding digital infrastructure: with the increasing digitisation of systems and processes, there are more potential entry points for cyber attackers to exploit.
- Financial incentives: cyber-attacks can be financially lucrative for attackers, who may seek to extort money through ransomware attacks or profit from selling stolen data on the dark web.
- Advanced hacking techniques: cyber attackers are constantly evolving their techniques, employing sophisticated methods such as ransomware, social engineering and zero-day exploits.
- Global connectivity: the interconnectedness of the internet allows cyber-attacks to occur across borders, making it difficult to trace and prosecute perpetrators.
- Lack of adequate security measures: some organisations may not prioritise or invest sufficiently in cyber security, leaving them vulnerable to attacks.

It is important for organisations and individuals to stay vigilant, maintain robust security practices, and adapt to the evolving threat landscape to mitigate the risk of cyber-attacks.

Russian Hack Group 'Black Basta'

Black Basta is a Russian hacker group that emerged in April 2022 and has gained prominence as a ransomware group since the beginning of 2023. They have been involved in a significant number of ransomware attacks, reaching a record-breaking 459 incidents of hacking and data leaks in March 2023, as reported by IT security company NCC Group.