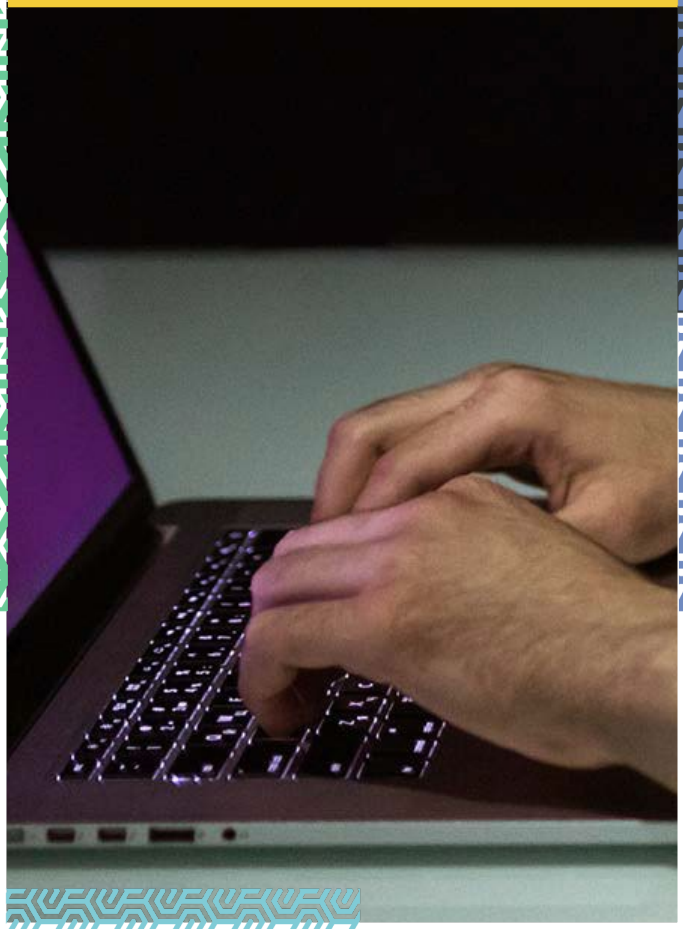
Risk control

Cyber Attacks



In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

Risk Management Partners
rmpartners.co.uk

Cyber Attacks

Introduction

Ransomware is a type of malicious software developed by those with criminal intent. If downloaded into IT systems, the software is programmed to lock the target's computer system or network, blocking access to important systems and data. The threat usually contained within ransomware attacks is that the locked information will be irrevocably damaged or destroyed if financial demands are not met within a prescribed timeframe.

In 2016 the UK started officially surveying company's and charities in order to assess how cyber security was persevered and prioritised in organisations within the UK. Trends in the statistics released in 2023 show a potential decline in the level of priority given to this area of risk[1].

In February 2020 a cyber-ransomware attack was carried out on a Borough Council in the North East of England. The attack rendered around 135,000 people without access to online public services[2]. The council's website and all computers and IT infrastructure were affected. Online appointment bookings, planning documents, social care advice and council housing complaints systems were among services that were no longer accessible. Frontline services continued with staff reverting to using pen and paper, with the council utilising social media platforms to communicate with the affected population[3].

In October 2020 a London Borough Council experienced a serious ransomware attack that paralysed many of its services[4]. Systems which residents used to pay rent and council tax, as well as accessing housing benefit payments were all affected. Months after the attack it was discovered that data stolen during the cyberattack has been published by the criminals responsible for the attack on the dark web[5].

The costs of coping with an attack and restoring systems can be very significant. The Wannacry ransomware attack that seriously affected the NHS several years before cost around £92m according to a Department of Health report[6]. The attack on the London Borough Council reportedly cost the council around £12m[7], whereas the attack on the Borough Council reportedly cost the organisation around £8.7m[8]. In the case of the Borough Council, they did eventually receive a support grant of £3.68m from the Government in connection with the costs incurred by the cyber-attack[9].

Double Extortion

One key feature to note about the London Borough Council ransomware attack was the demonstration of an evolving model for criminal attacks to steal data before encrypting the target's network. This has now become routine as a criminal practice. While there are potentially numerous network vulnerabilities, the main routes are through: remote desktop protocols; insecure virtual private networks; and devices with unpatched software or hardware.

The Targets

Targets for this new wave of ransomware attack include, but are not limited to, large public service providers such as council's, universities, hospitals and police organisations: organisations that are generally considered to have large available financial resources allied with little tolerance for service disruption due to the intrinsic value of the services provided.

Cyber Risk Management

The National Cyber Security Centre (NCSC) are primarily concerned with supporting the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, they provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

They very keenly promote a risk management approach to addressing cyber-security risk within all organisations, large and small, and recognise two closely related techniques that can assist organisations in approaching cyber-risk management: Component Driven and System Driven.

— Component Driven[10]

This technique offers benefits to organisations by assisting in addressing known technical vulnerabilities. For example, there may be a number of computers within an organisation that has been left unpatched or upgraded. A component-driven risk analysis can identify how the vulnerabilities in those computers could impact the organisation, as well as the steps needed to manage or eliminate those vulnerabilities.

— System Driven[11]

This technique is beneficial when managing large and complex systems. Although the individual components within the system may be working within precise expectations, cyber-security weaknesses may be created by the way in which these components interact with each other.

The NCSC also provides cyber-security guidance for public sector organisations which can be accessed **here.**

Summary

Events such as those detailed above can serve as reminders of the importance placed upon all organisations of the need to actively assess and manage cyber-security threats. It is clear that any organisation can become a target.

As we become more and more reliant on technology in our working lives, the importance of the need to implement, manage and review robust control strategies has never been clearer.

Risks evolve. And that includes cyber-risk. We may feel reasonably well protected today. But we must continually strive to ensure that we are not a cyber-security victim tomorrow.

References

1 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

2 https://www.bbc.co.uk/news/uk-england-tees-53662187

3 https://www.bbc.co.uk/news/technology-51504482

4 https://www.bbc.co.uk/news/uk-england-london-54606375

5 https://news.hackney.gov.uk/cyberattack-update/ [Accessed 25th November 2021]

6 https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

7 https://www.hackneycitizen.co.uk/2022/10/13/cyber-attack-recovery-hackney-council-12m/

8 https://www.bbc.co.uk/news/uk-england-tees-57433800

9 https://www.bbc.co.uk/news/uk-england-tees-56668176

10 https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches/understanding-component-driven-risk-management

11 https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches/understanding-system-driven-risk-management

Further information

Gallagher Bassett has a partnership arrangement with Broadgate Consultants for the provision of a Cyber Risk Health Check. This service falls outside of the elective day's arrangement and there is a fee payable for this service. The Health Check provides clients with a brief review of their current cyber protection levels and provides them with recommendations to strengthen their cyber resilience. The Health check itself will be a blend of meetings, an online assessment, a review of existing documentation and a final report presentation.

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

Get in touch

For more information, please contact your broker, RMP risk control consultant or account director.

contact@rmpartners.co.uk

Risk Management Partners

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk

FP1736-2023