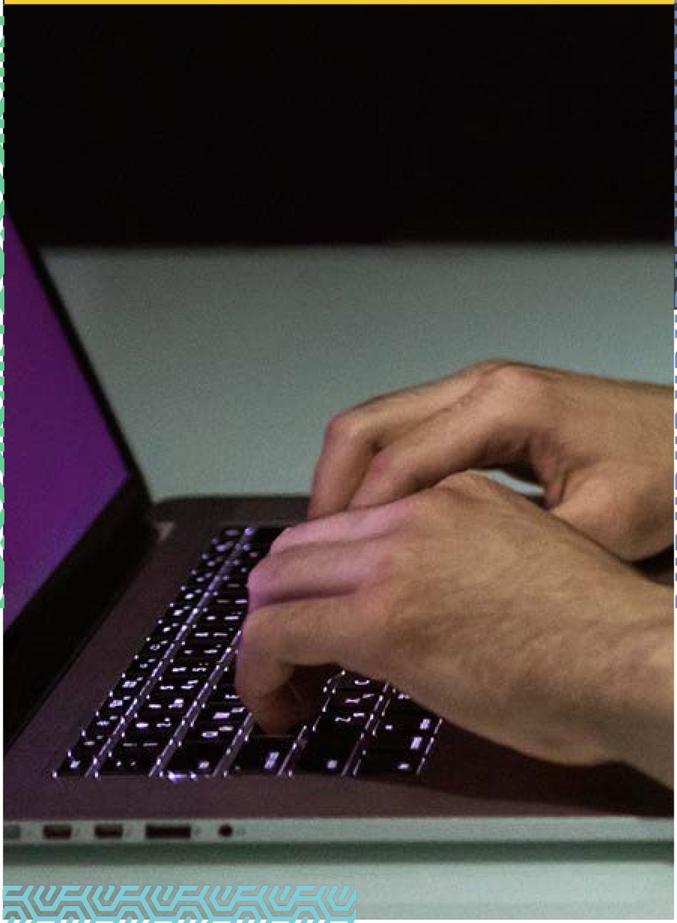
rmp

Risk control

Cyber Attacks



In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

Risk Management Partners
rmpartners.co.uk

Cyber Attacks

Introduction

In May 2019 a ransomware attack was carried out which resulted in the servers of the American city of Baltimore, Maryland being largely compromised by a new strain of ransomware called RobbinHood. Baltimore became the second U.S. city with a population of over 500,000 people to fall victim to ransomware in two years, after Atlanta was attacked the previous year [ref.1].

In the UK the National Cyber Security Centre (NCSC) stated that it responded to 777 incidents in the period September 2020 to August 2021, 20% were linked to the health sector and vaccines [ref.2].

Some of the incidents involved public authorities with one local authority being hit by a ransomware attack in which the hackers scrambled files and demanded money. This led to a number of council services, including payment systems, being paralysed and unavailable with some key services unavailable for a number of weeks. This required the authority to undertake a series of remedial actions, including the building of a new server and website, and mobilising a temporary call centre.

The costs of coping with an attack and restoring systems can be significant and it is reported that the Wannacry attack in 2017 cost the NHS around £92m [ref.3].

Ransomware is a type of malicious software developed by those with criminal intent. If downloaded into IT systems, the software is programmed to lock a target’s computer 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 demands are not met within a prescribed timeframe.

Double Extortion

One key feature to note about 2020 was an evolving model for criminal attacks to extract data before encrypting the victim network; threatening to leak the data extracted unless a ransom was paid. This has now become routine as a mode of attack. While there are numerous network vulnerabilities the main routes are through: remote desktop protocols; insecure virtual private networks; and devices with unpatched software or hardware.

This form of hack is a growing problem for large targets like public authorities and companies. Jeremy Fleming, Director at GCHQ states that “the world changed in 2020 and so did the balance of threats we are facing.” [ref.4]

The Target

Specific targets for this new wave of ransom attack are large public service providers such as universities, hospitals and police departments; organisations that have large incomes, but no scope for going off-line for days or weeks to invoke structured IT disaster recovery procedures.

However the major significance of ransomware attacks in the public sector is the immediate disruption caused to municipal services as residents may not be able to access important information, pay taxes, fees, or fines online, report potholes or make complaints via the organisation’s website. The financial consequences of a cyber-attack can be far greater than the ransom demand and for many organisations it can seem expedient to pay the hackers and quickly restore services, but the National Cyber Security Centre (NCSC) warns that this is fraught with pitfalls and a solution that should be avoided [ref.5].

Cyber Risk Management

The NCSC outlines that “the establishment of predetermined security risk management structures, business processes, roles and requirements are too often separated from the normal decision making structures and processes used elsewhere in the business. This separation can lead to uncertainty, delays and confusion in the technology decision making process of the problems.” but that there is “no 'one size fits all' approach to governance that can work for every organisation.” [ref.5].

For this reason the NCSC, which offers a range of guidance specifically for public sector organisations, including ‘The 10 Steps to Cyber Security’, believe that “adopting security measures tailored to your situation, but which align with the 10 steps, will help protect your organisation from cyber-attack” [ref.6].

However there is also a need for organisations to understand what they are protecting themselves against and to help with this the NCSC have produced a white paper entitled, ‘Common Cyber Attacks: Reducing The Impact’ which sets out what a common cyber-attack looks like and how attackers typically undertake them [ref.6].

Summary

Events such as those detailed above serve as reminders of the importance of the need to actively risk assess cyber security threats, with robust control strategies implemented and maintained to protect our organisations from the continuing threat posed by the methods of modern-day criminality.

Four in ten businesses (39%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months. Like previous years, this is higher among medium businesses (65%), large businesses (64%) and high-income charities (51%) [ref 9].

As a final sting in the tail there is a requirement under the General Data Protection Regulation 2018 for all UK companies, including Local Authorities, to report data breaches to the Information Commissioner's Office (ICO) within 72 hours. Failure to do so can result not only in in heavy fines and penalties but also reputational damage while exposing the organisation to civil claims. [ref.8].

References

1 BBC (2019), Baltimore ransomware attack: NSA faces questions. [ONLINE]. Available at:

https://www.bbc.co.uk/news/world-us-canada-48371476

[Accessed 25th November 2021]

2 BBC (3RD Nov 2020), UK cyber-threat agency confronts Covid-19 attacks ack. [ONLINE]. Available at:

https://www.bbc.co.uk/news/technology-54782258

[Accessed 25th November 2021]

3 The Telegraph (2018), WannaCry cyber-attack cost the NHS £92m as 19,000 appointments cancelled. . [ONLINE]. Available at:

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

[Accessed 25th November 2021]

4 National Cyber Security Centre, part of GCHQ: Annual Review 2021. [ONLINE]. Available at:

https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021

[Accessed 25th November 2021]

5 The National Cyber Security Council, Risk Management Guidance. [ONLINE]. Available at:

https://www.ncsc.gov.uk/collection/risk-management-collection/governance-cyber-risk/security-governance-enabling-sensible-risk-management-decisions-communication

[Accessed 25th November 2021]

6 The National Cyber Security Council, 10 Steps to Cyber Security. [ONLINE]. Available at:

https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

[Accessed 25th November 2021]

7 BBC (2019). More than half of British firms 'report cyber-attacks in 2019'. [ONLINE]. Available at:

https://www.bbc.co.uk/news/business-48017943

[Accessed 25th November 2021]

8 Information Commissioner's Office. Guide to the General Data Protection Regulation (GDPR). [ONLINE]. Available at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

[Accessed 25th November 2021]

9 Cyber Security Breaches Survey 2021 [ONLINE]. Available at:

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

[Accessed 29th November 2021]

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

This newsletter does not purport to be comprehensive or to give legal advice. While every effort has been made to ensure accuracy, Risk Management Partners cannot be held liable for any errors, omissions or inaccuracies contained within the document. Readers should not act upon (or refrain from acting upon) information in this document without first taking further specialist or professional advice.

Risk Management Partners Limited is authorised and regulated by the Financial Conduct Authority. Registered office: The Walbrook Building, 25 Walbrook, London EC4N 8AW. Registered in England and Wales. Company no. 2989025.