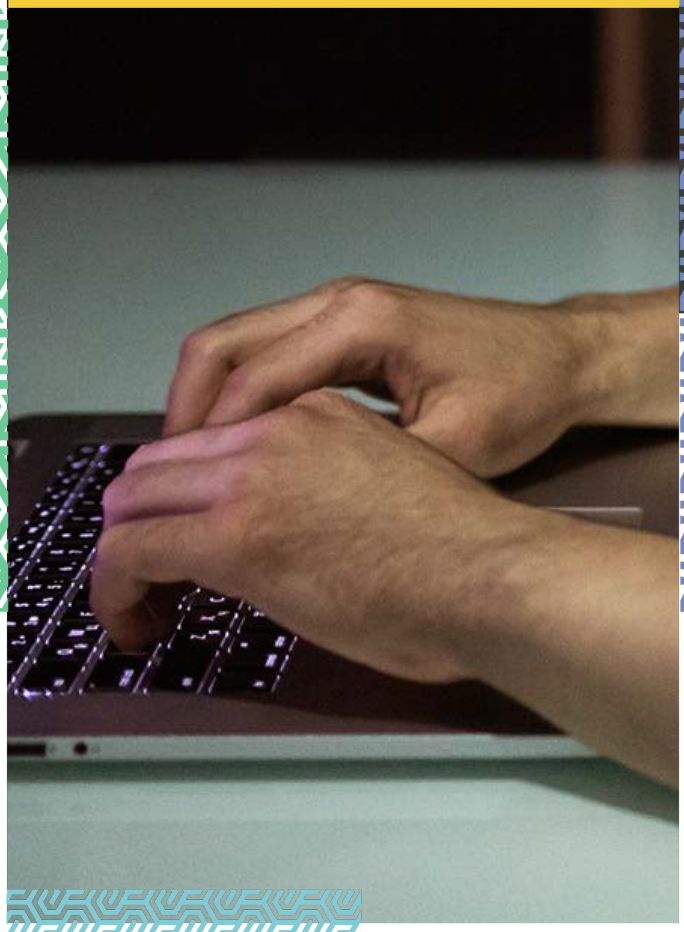
Risk control

Cyber Attacks



In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

Risk Management Partners
rmpartners.co.uk

25 YEARS OF DEDICATION IN ACTION

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 (BBC, 2019 / USA Today, 2018)

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 the demand is not met within a prescribed timeframe.

Although ransomware demands tend to be relatively small in comparison to the financial standing of the target organisation, the sum involved in the Atlanta attack was reported to be $51,000 *(O'Donnell, L. 2018)*, the costs of coping with an attack and restoring systems can be significant. It is reported that the Wannacry attack in 2017 cost the NHS around £92m (The Telegraph, 2018)

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.

But the major significance of ransom 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.

Summary

Events such as these serve as reminders of the importance of the need to robustly protect our organisations from the continuing threat posed by the methods of modern-day criminality.

Research by the insurer Hiscox suggested that 55% of UK firms had experienced a cyber-attack in 2019, up from 40% in the previous year. It also reported that average losses from breaches also soared from $229,000 to $369,000, an increase of 61% *(BBC, 2019)*.

Under the General Data Protection Regulation 2018 (GDPR) all UK companies including local authorities are required to report data breaches to the Information Commissioner's Office (ICO) within 72 hours. Failure to do so can result in heavy fines and penalties.

References

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

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

[Accessed 4 November 2019]

2 USA Today (2018). Atlanta ransomware attack: Employees told not to turn on computers. [ONLINE]. Available at:

https://www.usatoday.com/story/tech/2018/03/23/atlanta-hit-ransomware-attack-city- employees-told-not-turn-computers/452846002/.

[Accessed 4 November 2019]

3 O'Donnell, L. (2018). *Ransomware Attack Cripples Several Atlanta City Systems*. [online] Threatpost | The first stop for security news. Available at:

https://threatpost.com/ransomware-attack- cripples-several-atlanta-city- systems/130739/

[Accessed 4 November 2019]

4 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 4 November 2019]

5 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 4 November 2019]

6 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 4 November 2019]

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 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

FP1261-2019