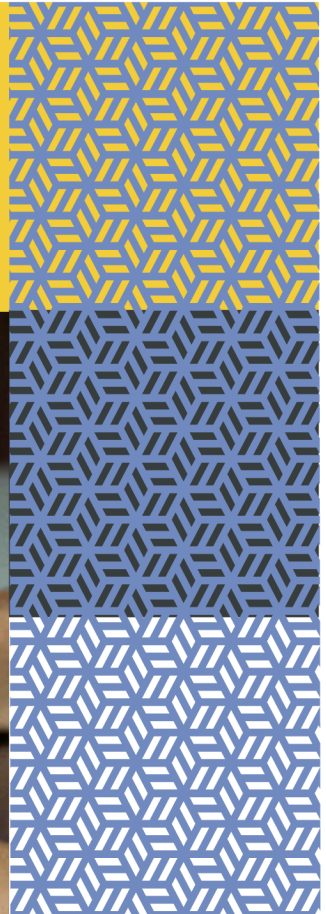
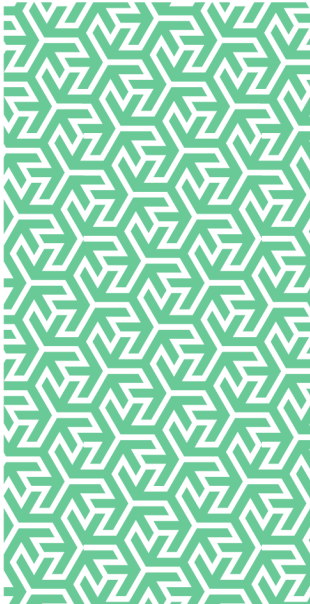


rmp

**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 March 2018 a ransom-ware attack locked out the City of Atlanta's municipal government staff from their computer systems. This attack was described as one of the most sustained and consequential cyber-attacks ever mounted against a major American city administration (Weise, 2018).

Ransom-ware 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 ransom-ware attacks is that the locked information will be irrevocably damaged or destroyed if the demand is not met within a prescribed timeframe.

Ransom-ware demands tend to be relatively small in comparison to the financial standing of the target organisation. For example, the sum involved in the Atlanta attack was reported to be \$51,000 (O'Donnell, L. 2018).

## The Target

A 2016 survey of Chief Information Officers in the USA found that obtaining ransoms was the primary motivation for nearly one third of all attacks on a city or county government. Fewer than half of the local governments surveyed reported a formal cyber-security policy was in place. (ICMA, 2018)

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.

Based on Freedom of Information requests, Big Brother Watch found that UK local authorities have experienced in excess of 98 million cyber- attacks over five years. At least one in four councils experienced some form of cyber security breach between 2013 and 2017 (*Big Brother watch, 2018*).

Local authorities will be required to report breaches of the rights and freedoms of individuals to the Information Commissioner's Office (ICO) under the 2018 General Data Protection Regulation (GDPR).

## References

- 1 USA Today. 2018. *Atlanta hit by ransomware attack, city 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 13 April 2018]
- 2 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 13 April 2018]  
[https://icma.org/sites/default/files/309075\\_2016%20cybersecurity%20survey\\_summary%20report\\_final.pdf](https://icma.org/sites/default/files/309075_2016%20cybersecurity%20survey_summary%20report_final.pdf)
- 3 Cybersecurity 2016 Survey. (2018). [ebook] Maryland: ICMA. Available at:  
[https://icma.org/sites/default/files/309075\\_2016%20cybersecurity%20survey\\_summary%20report\\_final.pdf](https://icma.org/sites/default/files/309075_2016%20cybersecurity%20survey_summary%20report_final.pdf)  
[Accessed 16 April 2018]
- 4 Cyber attacks in local authorities. (2018). [ebook] Big Brother Watch. Available at:  
<https://bigbrotherwatch.org.uk/wp-content/uploads/2018/02/Cyber-attacks-in-local-authorities.pdf>  
[Accessed 16 April 2018]

## 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](mailto:contact@rmpartners.co.uk)



### **Risk Management Partners**

The Walbrook Building  
25 Walbrook  
London EC4N 8AW

020 7204 1800  
[rmpartners.co.uk](http://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.