Cyber Risks & Liabilities

September/October 2019

Ransomware Attacks Are on the Rise: Prevention Tips

While cyber-incidents of any form are a rising concern for organisations in the UK, recent research revealed that a specific type of attack is escalating at an alarming rate: ransomware. This malicious software typically invades a victim's device through disguised downloads or email attachments, disables the device's anti-malware software and lays dormant until activated by the cyber-criminal who created it. Once activated, the ransomware is able to encrypt every file on the device and force the victim pay a ransom—often with cryptocurrency (eg bitcoin)—to have their files properly restored.

The UK was the biggest global target for ransomware attacks in the first half of 2019—with **the number of ransomware incidents increasing by 195 per cent** when compared to last year's totals, according to SonicWall. What's worse, ransomware attacks are known to result in more costly consequences than the average cyber-incident due to the additional risk of having to pay a ransom to restore stolen data.

Consider the following guidance to keep your organisation from becoming another statistic and the next victim of a ransomware attack:

- **Software updates**—It's vital to routinely update your cyber-security software (eg firewalls, anti-malware or anti-virus software) on all devices to properly protect against ransomware.
- **Staff training**—Be sure to provide routine cyber-security training for all employees to ensure they are capable of reducing ransomware risks. Specifically, employees should know how to detect phishing scams to prevent ransomware from invading organisational devices through email attachments.
- **Device controls**—Consider implementing a security feature on all workplace devices that filters employees' web browsing traffic and blocks malicious websites. This will help prevent the risk of employees accidentally downloading ransomware.
- **Back-up systems**—In order to decrease your vulnerability during a ransomware attack, establish a secure back-up location for storing data. Doing so will protect you from having to pay a costly ransom if your devices are compromised.
- **Response planning**—To help limit the consequences of a potential cyber-attack, create a cyber-incident response plan and test the plan regularly with staff for effectiveness.

More than anything, you need cyber-insurance to ensure ultimate peace of mind against the growing threat of a ransomware attack. For more information, contact Crendon Insurance Brokers Ltd today.

Crendon
Insurance
Brokers

Crendon Insurance Brokers Ltd
The CIB A Building, 146 Hagley Road, Edgbaston
Birmingham, West Midlands, B16 9NX
0121 45 45 100
www.crendoninsurance.co.uk
enquiries@crendoninsurance.co.uk

Are Your Past Employees Still Holding on to Company Data?

Restricting access to company data is an important practice within any organisation to reduce the risk of lost, damaged or stolen data. Indeed, your organisation should have systems in place to only allow trusted, competent employees access to sensitive information. But what happens when those employees leave their positions?

Following an incident with two former Metropolitan Police Service (MPS) officers, the Information Commissioner's Office (ICO) recently released a statement regarding the ramifications of employees retaining organisational data after leaving their role. Although the ICO decided not to take formal regulatory action, an investigation revealed that the MPS officers acted unlawfully under the GDPR by sharing sensitive information with the media about a case they worked on after they had left their positions.

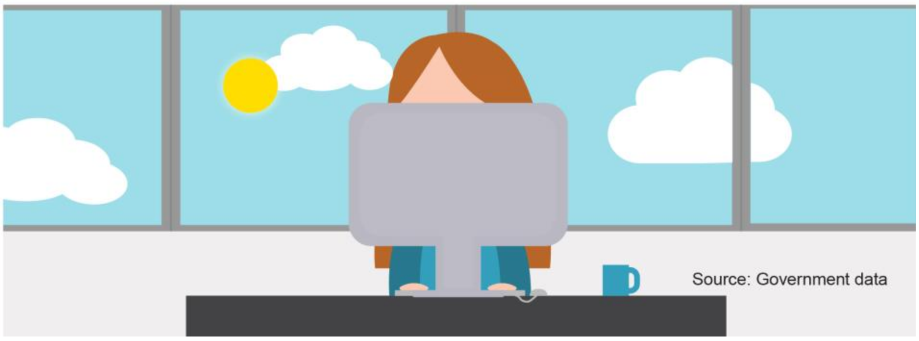
While the MPS officers did not receive a regulatory consequence for their actions, it's important to note that former employees who 'knowingly or recklessly' hold on to sensitive company data without your consent after leaving their role could face significant GDPR fines.

Further, your organisation could be held liable under the GDPR for its former employees' poor practices as well, if you don't take reasonable efforts to ensure these employees no longer receive access to sensitive company data.

With this in mind, be sure to warn employees of the consequences that could arise from retaining company data after leaving your organisation. Doing so could help protect both your organisation and past employees from severe GDPR non-compliance concerns.

Is Your Workforce Prepared for the Digital Skills Demand?

An estimated 90% of job roles will require some degree of digital skills by 2040.



Source: Government data

Use This Guidance to Reduce Your Firm's Digital Skills Gap Problem

Workplace technology continues to evolve every day. And as companies across industry lines join in the race to 'go digital', it's vital now more than ever for your organisation to possess a skilled workforce that is capable of utilising the latest technology.

Nevertheless, recent data found that many UK firms are suffering from a digital skills gap. As a result, these organisations are unable to reap the wide range of benefits that come with integrating advanced, readily available technology in the workplace—including increased productivity levels, a lowered risk of human error and the ability to better service customers.

What's worse, **this skills gap concern has cost the UK economy £500 million in the last 12 months alone**, according to a recent government report. Put simply, your organisation can't afford to continue suffering from a digital skills gap problem. Use these tips to reduce your risks:

- **Consult the IT department**—Be sure to include your firm's technology experts when discussing an approach to combat digital skills gap concerns. These employees will likely have unique, innovative ideas for helping other staff bolster their digital skill set.
- **Offer apprenticeships**—By investing in an apprenticeship programme, your organisation will be able to help young employees harness their digital skill set early on. This practice will also help further incorporate cyber-skills into your organisation's employee induction process.
- **Provide routine training**—Cyber-training shouldn't be limited to the apprenticeship programme or induction process. Make sure employees receive routine training on digital skills, regardless of how long they have worked for your organisation. This training is especially important when your workplace implements new technology or software, as organisational processes might change.
- **Create a culture of growth**—Above all, your organisation should take steps to promote a culture that emphasises the importance of continuous learning and technological growth. Doing so will keep employees motivated to learn digital skills and better adapt to new workplace technology.

Crendon Insurance Brokers