A blurred photograph of a city street scene, showing pedestrians and a car in motion, with a building facade in the background. A yellow geometric pattern is overlaid on the right side of the image.

Cyber risk at a glance

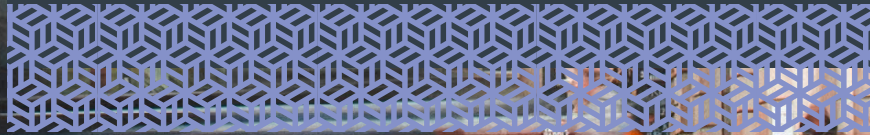
The scale and frequency of cyber-attacks in the UK is increasing year on year.

Last year, councils reported 700 data breaches to the Information Commissioner's Office (ICO). Up 10% from 2019.

Cyber Insurance still remains a misunderstood product.

Exposure to cyber risk can cause business interruption, income loss, large scale data breaches of sensitive information, possible reputational damage, and at its worse 'injury', with some or all of these risks not being covered by traditional insurance covers.

For example, it may well be the case that your public liability policy won't cover non-physical damage to a third party caused by data theft.

A decorative border at the bottom of the text area featuring a repeating blue geometric pattern of interlocking lines.



Do you really need cyber insurance?

There can be little doubt that the frequency and severity of cyber-attacks in the UK remains a major concern. According to the UK Government's Cyber Security Breaches Survey 2020, 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%).

The picture for local authorities in the UK is just as concerning. According to a recent Redscan report, councils reported two data breaches per day to the Information Commissioner's Office in 2020.

A large and growing threat emerging in the UK is that of ransomware - where cyber criminals encrypt networks and demand a ransom to release the data. Ransomware attacks have increased over 150% in the first half of 2021 compared with the same period in 2020.

Hackney Council was the most high-profile ransomware case, where critical services were forced to shut for several weeks. Redcar and Cleveland Borough Council suffered a cyber-attack that shut off key services to over 135,000 residents, and was reported to have cost the council over £10m.

Cyber-attacks on local authorities most commonly involve viruses and other malicious software, or phishing, where the perpetrator attempts to obtain sensitive information such as passwords.

Then of course, there are the ramifications that exposure to these risks can cause, such as business interruption, income loss, damage management and repair, and the possibility of reputational damage if IT equipment or systems fail or are interrupted.

The huge value that cyber insurance policies bring is not just the financial indemnity, but access to specialist advisors. Including IT Forensic specialists, law firms who specialise in GDPR and data privacy, and PR specialists who can help organisations navigate the impact a cyber attack has on their reputation.



Coverage uncertainty

Unfortunately, there can be a degree of uncertainty for risk managers as to what exactly their current insurance policies provide in terms of coverage. Specifically, whether you would be covered in the event of a cyber-attack on your organisation.

Historically, from an insurance perspective, we have tended to look at coverage initially from the point of view of tangible assets, such as physical buildings, plants and machinery, with available extensions in the form of business interruption cover for loss of revenue.

And yet, the world is changing. Whereas historically, and rightly, a company or public authority's focus would have been on its physical assets, in the 21st century there can be little argument that intangible assets - your information, your data, and your intellectual property - are just as important.

As we know, cyber-attacks can target any form of electronic information, so we are clearly not in the realm of tangible assets. Instead we are looking at a variety of scenarios, including loss or damage to data or software programmes; business interruption losses as a result of network downtime; or even cyber & data extortion demands where third parties threaten to damage or release data if money is not paid to them. We've moved from a tangible to an intangible risk.

For example, a party could hack into your computer systems and cause extensive damage, but if you haven't taken out cyber insurance then you will not necessarily be covered for the consequences of such an attack. It's vital to ensure that your intangible assets are insured, but the good news is that cyber insurance market is developing to plug that gap.

What about public liability?

You might think that your public liability (PL) insurance will insure you for the consequences of a cyber-attack, but PL in the traditional sense covers bodily injury or physical damage to a third party. From a cyber perspective, if something from a local authority causes non-physical damage to a third party, it won't be covered.

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

<https://www.redscan.com/media/Disjointed-and-under-resourced-cyber-security-across-UK-councils-A-Redscan-FOI-Analysis-report.pdf>

<https://www.bbc.co.uk/news/uk-england-london-55574580>

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

In some respects, cyber insurance at the moment is like the directors & officers' liability market was some years ago, with limited knowledge about what the product covers and why it's so important. And yet, with the scale and regularity of cyber-attacks in the UK increasing year on year, it's vital that you review the adequacy of your existing insurance and determine whether it will cover you in the event of an attack on your authority.

Need to know more?

At RMP we have a partnership with one of the UK's leading providers of cyber insurance, PEN Underwriting, and we'd be happy to talk you through the scope of cyber cover in detail.

Get in touch

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

Risk Management Partners
contact@rmpartners.co.uk

67 Lombard Street
London EC3V 9LJ

020 7204 1800
www.rmpartners.co.uk

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

This article and related document links do 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 article and related document links. Readers should not act upon (or refrain from acting upon) information in this article and related document links without first taking further specialist or professional advice.



Dedication in action