Commercial Insurance Profile

June 2020

Organisations that experienced a cyber-attack in 2019-20 reported the following most common forms of attack:

86% experienced a phishing attack (up from 72% in 2017).

26% experienced impersonation incidents.

19% experienced malware mishaps (including ransomware).

Source: The Department for Digital, Culture, Media & Sport

Provided by:
MacKay Corporate Insurance

MACKAY
Corporate Insurance Brokers

Revealed: Government Releases the Latest Cyber-security Statistics

Since 2016, the Department for Digital, Culture, Media & Sport has used the annual Cyber Security Breaches Survey to track trends related to cyber-security and breaches.

The latest findings in the 2020 survey indicate that cyber-attacks are becoming not only more frequent, but also more sophisticated.

According to data collected by the survey, 46 per cent of all UK businesses reported having a breach of cyber-security or having suffered from an attack in the last 12 months. The rate increased to 68 per cent and 75 per cent for medium and large businesses, respectively.

Of the businesses that suffered a breach or attack, 32 per cent said that they had to deal with an issue on a weekly basis. In 2017, only 22 per cent of victimised respondents reported that level of frequency.

The most recent survey also shows that the types of cyber-attacks that businesses need to be aware of continue to change. Since 2017, the proportion of businesses that suffered a breach or attack, and experienced phishing attacks has increased to 86 per cent, while those having issues stemming from malware has dropped to 17 per cent.

Cyber-threats are constantly evolving, so your defences must do so as well. According to survey results, 51 per cent of businesses update their senior management on cyber-security at least once per quarter.

Some general cyber-security methods that more businesses have implemented in recent years include:

- Seeking out information and guidance
- Carrying out cyber-security risk assessments
- Having employees whose roles specifically include information security and governance
- Having written cyber-security policies
- Backing up data on cloud servers

Still, there are many businesses that may be at risk. Only 15 per cent of respondents said that they had reviewed cyber-security risks presented by suppliers, and only 32 per cent reported that they are currently insured in some way against cyber-risks.

According to survey results, the average cost of all cyber-security breaches reported by businesses in the previous 12 months was £3,320, with the amount rising to £5,220 for medium and large organisations. A cyber-attack can devastate your organisation's finances, reputation and future, so it is important to take these threats seriously. Contact us today to learn more about how you can protect your business.

The Importance of Data Protection Compliance

A **data breach** can already be an extremely costly incident, but organisations also must be aware of the **penalty** for being non-compliant with data protection laws, such as the General Data Protection Regulation (GDPR).

Failure to comply with the GDPR can carry a maximum fine of nearly

£17.5 million

or **4% of your annual global turnover**—whichever is greater.

Supreme Court Rules on Employer Liability for Data Breaches

On 1st April 2020, the UK Supreme Court ruled in Various Claimants versus WM Morrisons Supermarkets that the employer was not vicariously liable for a data breach caused by a former employee.

In 2014, the employee posted personal details of nearly 100,000 Morrisons employees online. A class action lawsuit alleged that the company was directly or vicariously liable for the breach.

The High Court found that Morrisons was vicariously liable for the breach, but did not have direct liability for the breach due to the employee having acted independently. Under established law, an employer is vicariously liable for actions committed by an employee who is acting within their 'field of activities'.

Upon appeal, the Supreme Court found that the employee was not acting within their regular 'field of activities', but rather carrying out a personal vendetta. As such, the Court's ruling absolved Morrisons of vicarious liability for the data breach.

Although the Supreme Court's decision may reduce the likelihood of group litigation stemming from data breaches, employers should still take every possible precaution to implement strong cyber-security measures and protect their employees' data—especially in the era of the General Data Protection Regulation.

Do You Know the Key Benefits of Equipment Breakdown Insurance?

Organisations across industry lines rely on a wide range of technology and machinery to conduct key operations. With this in mind, any equipment breakdown incident could carry severe consequences. That's why having robust equipment breakdown insurance is crucial.

At a glance, equipment breakdown cover offers protection in the event of any workplace equipment malfunction or failure. Some key benefits of having an equipment breakdown policy include:

- **Repair and replacement compensation**—After a breakdown, your policy will cover repair or replacement costs for damaged equipment—including time and labour.
- **Lost income protection**—If a breakdown keeps your business from making money, your policy will provide compensation until the equipment is fixed or replaced.
- **Spoilt inventory reimbursement**—If a breakdown leaves you with spoilt inventory, your policy will cover the cost of replacing the perishable items.
- **Additional expense assistance**—If a breakdown results in any other restoration-related expenses for your organisation, your policy will offer reimbursement.

Contact us today to discuss bespoke equipment breakdown cover solutions.