Risk insights
Cyber Insurance

Macbeth

What is Cyber Insurance?

Almost every business holds valuable information, from payment details and employee data to medical records and supplier agreements. So, it's unsurprising there's been an increase in cybercrime in recent years, with cybercriminals now going to extreme lengths to steal sensitive data, and exploit individuals and businesses for their own financial gain.

The majority of cyber incidents are the result of human error (clicking on a phishing email, using a weak password or simply failing to apply a security update) and as cybercriminals adopt increasingly sophisticated techniques, a fraudulent third party trying to access your system is becoming a lot harder to spot.

Cyber insurance offers protection against the attacks you hope won't happen. It covers financial losses that might arise from a cyber-attack, including data breaches, system damage, loss of income, and even cyber extortion (covering investigation costs and ransom payments).

All businesses that use digital systems (e.g. sending or receiving payments, or simply using email) are vulnerable to a cyber-attack, and the fact that technology and data are fundamental to doing business in the modern world, make cybercrime a very real and evolving threat.

Who needs Cyber Insurance?

Whatever line of business you're in, there's a growing reliance on the internet and technology, and if your business handles sensitive or confidential data, then you need the protection that Cyber Insurance offers.

Businesses of every scale, whether start-ups, SMEs, or large corporations, face the looming threat of cyber-attacks. In the vast landscape of cybercrime, most attacks aren't tailored to a specific target; rather, cybercriminals cast a wide net, using diverse tactics like malware, ransomware, and social engineering. This indiscriminate approach renders any business, regardless of its size or industry, vulnerable to an attack.

And if you don't know how you would respond when it 'goes dark' and you find yourself locked out of your I.T system and facing a ransom demand, the consequences could be devastating.

Jargon busting

Cyber-attack
Any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device.

Cybercrime
Criminal activities carried out using digital devices and/or networks, including fraud, identity theft, data breaches and scams.

> When it comes to Cyber, humans will always be the weakest link. The evolving landscape of cyber threats means attackers are finding new ways to exploit human error, so it's best practice to assume every contact has the potential to pose a threat. Trust your gut, and if something seems off, it probably is.
>
> **Suzanne Fowler,** Client Manager

Navigating the unpredictable: The reality of cyber threats

The increased digitalisation of our world is an undeniable reality. However, alongside the numerous advantages the digital age offers, it also provides criminals with unprecedented opportunities to exploit businesses for their own financial gain.

As such, it's never been more important for businesses to stay vigilant and informed about the cyber threats they are likely to face.

Did you know?

Most cyber-attacks are opportunistic. This means any business, large or small, can be targeted, with 32% of UK businesses suffering a cyber incident in the last 12 months*.

1 in 5 UK businesses have been a victim of a cyber-attack in the last 12 months.[1]

and

34% of the businesses who experienced a cyber-attack or breach in the last 12 months ended up being victims of a cybercrime[2]

54% of UK businesses, regardless of their size, say that loss of data or a data breach is their number-one concern[1]

yet

Aviva estimate **16% of SMEs didn't know cyber insurance even existed**[3]

The thief's toolkit – the most common cyber-attack methods

Even with the best IT security in the world, your business will never be 100% protected from cyber threats.

Read that again.

Cybercriminals are the 21st century burglars, looking to use any means necessary to force their way into your business and take your valuables. These are the three most common cyber-attack methods lurking in the shadows:

Malware
Harmful software, such as viruses, worms and spyware, which can steal information and cause system disruption, leading to financial loss and business downtime.

Ransomware
A type of malware that encrypts files and demands payment for decryption, causing system disruption and financial loss. Increasingly, these attacks are also leading to exfiltration of data, with a threat to release or publish the data unless certain demands are met.

Social engineering scams
Deceptive techniques used to manipulate individuals into divulging confidential information or making a payment to fraudsters, causing data breaches and financial loss.

[1] Aviva Cyber Report 2024.

[2] Cyber Security Breaches Survey, 2023, DCMS.

[3] SME Pulse survey conducted by YouGov, on behalf of Aviva, in which 512 British SMEs were questioned. Fieldwork took place between 5-12 October 2022.

* Cyber Security Breaches Survey, 2023, DCMS.

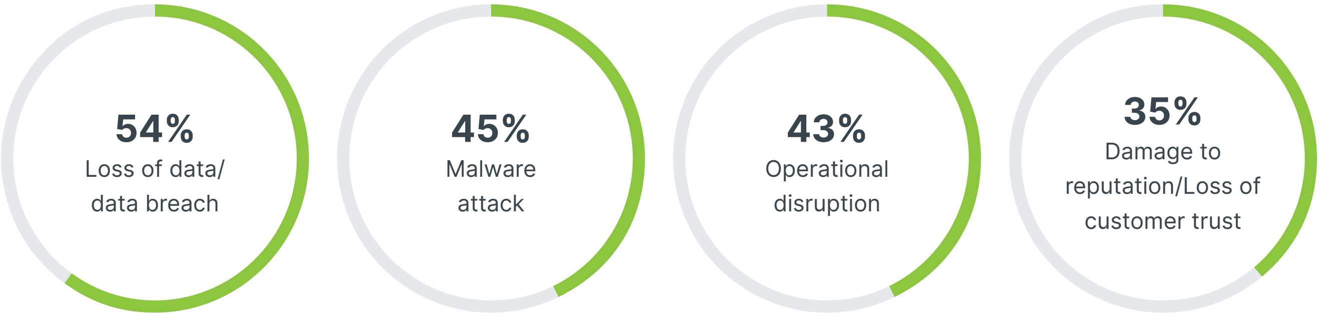
What are businesses most worried about?

A cyber-attack can leave a business extremely vulnerable, with loss of data or a data breach being the number one worry for most businesses (54%), regardless of their size.

Data can have a direct impact on the day-to-day running of a business, not to mention regulatory penalties for not managing data or a data breach correctly.

Malware was the second-largest concern for small businesses (45%), with operational disruption rated higher for mid-market and large corporates.

Modern businesses are increasingly vulnerable to attacks due to their interconnected systems, and the loss of any system could have potentially wider impacts across the business or for customers.

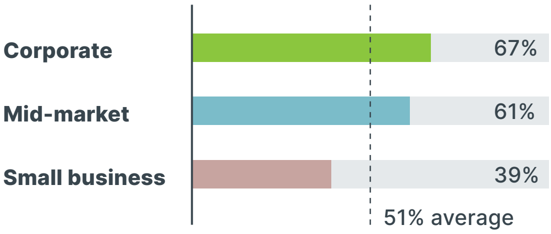


Would you know what to do if the worst happened?

If your business suffered a cyber-attack tomorrow, would you know what to do? Just 51% of all businesses felt sure about what to do in the event of an attack. And while larger companies feel more confident in their ability to react, just two in five small business owners felt they would choose the right action if their systems were breached.

Cyber Insurance is critical for every business, providing you with the immediate support you need to minimise any damage - and get your business back on track.

Cyber Insurance is more than just cover for financial loss, it holds your hand during and after an attack, giving you expert advice and support when you're at your most vulnerable.



Key fact

The first hour of a cyber-attack is known as the 'golden hour' – where effective action can dramatically reduce the impact of the incident. This is particularly important if you don't have systems in place to take the necessary actions on your own.

Source: Aviva Cyber Report 2024.

Industry vulnerability: Assessing Risks Across Sectors

Cyber-attacks can affect any business, of any size, in any industry, resulting in a potentially devastating impact on everyday operations, finances, reputation, and compliance.

Manufacturing

Reliance on continually evolving technology makes this sector particularly vulnerable, with processes at risk of being severely disrupted if system software if attacked. This could lead to production being halted, leading to potential loss of revenue or contractual penalties.

This sector is also at risk of loss of intellectual property.

Did you know?

Healthcare data can be more valuable on the dark web then personal information, making it a key target for cybercriminals.

Professional Services and Technology

Professional Services are particularly vulnerable to cyber-attacks as they handle sensitive data, as well as money on behalf of clients. There's also a growing trend for targeting law firms' commercial and residential property teams to steal customer funds, potentially leading to loss of customer trust. The Technology industry is very dependent on digital solutions making it particularly vulnerable, especially if connected devices are hacked and a ransomeware attack is launched, which could lead to large losses.

Construction

These firms hold a large amount of confidential and highly sensitive information like employee data, tenders and property proposals, which if exploited could lead to firms suffering financial losses. Construction firms often use software with multiple users (architects, contractors and planners) meaning there are more opportunities for exposure, which could lead to a breach of data, reputational damage, and possible loss of contracts.

Motor industry

Cybercriminals might target motor traders to gain access to their customers personal data (which could be quite detailed if the customer has taken out car finance as part of a sale). Stolen data can then be sold to make money, and cybercriminals might block access to computer files until a ransom is paid or use scams to steal funds from bank accounts.

Health and Public Sector

Often reported in the news, these are two of the most exposed industries, due to the vast amount of confidential and sensitive data they hold. Their open systems are easily infiltrated, for example a hacker might attack the vulnerable computer system of a supplier who has full access to a healthcare provider's patient data. A data breach could also have devastating repercussions, such as patients data not being accessible in a hospital setting, and heathcare providers could be left open to fines and penalties under data protection legislation.

Property Owners

This sector is vulnerable to cyber threats due to the amount of personal information held by businesses (contracts, and digital payments exchanged between agents, landlords and tenants). If this information is obtained by a cybercriminal, they may carry out identify theft to forge documents like passports, or carry out mortgage fraud where fake identity documents are used to sell or remortgage a property for their own financial benefit.

What can I do to be more 'cyber aware?'

Cyber-crime can feel overwhelming. Afterall, it's yet something else to think about and it can be quite a complex subject. So, where do you start? The good news is there are lots of simple actions you can take right now to reduce your risk of a security breach or attack.

How cyber savvy are you?

Take our free 2 minute quiz today and get your results instantly.

Speak to your broker

Whether you're a newbie to Cyber Insurance, or you'd like to increase your level of cover, your broker has the expertise to provide you with the most cost-effective option that caters to your specific cyber needs. Cyber-attacks can result in tangible losses to your business (data, income, money) and/or liability claims from employees or third parties, so when it's time to evaluate your cyber risk, you need to consider the overall impact an attack could have. Your broker should ask you the right questions to work out how exposed your business is to a cyber-attack, the potential consequences of that risk, and how you can prevent it.

Educate your teams

Human error accounts for the majority of cyber-attacks, so it makes sense to do everything you can to lessen the risk, or you could end up being the weakest link in your cyber security. Start talking to your teams about cybercrime, and bear in mind if you have remote workers, they're seen as easy targets because they are unlikely to have the same level of security protections as employees in an office setting. A combination of cyber insurance **AND** taking time to train your team will help you feel more in control. Test your employees with mock phishing emails (phishing is the most common cause of cyber-attacks) and look out for news-jacking where hackers send timely and topical scams that feel 'relevant' (making you more likely to click on them).

Practice good cyber-hygiene

With cyber-attacks becoming more frequent and severe in today's business climate, it's never been more important to use good cyber-hygiene practices that minimise your exposure to digital threats.

- ✓ **Passwords** – Make them strong (like a good cup of tea) and avoid sharing or using them across different accounts.
- ✓ **Multifactor Authentication** – Important accounts (email, social media and banking) should require multifactor authentication to limit the opportunity for cybercriminals to steal confidential data.
- ✓ **Data Backups** – Critical business files should be backed up in a separate secure location like an external hard drive or within the cloud.
- ✓ **Security Software** – A high-quality antivirus programme can perform automatic device scans to detect and remove malicious software, providing protection from online threats.

macbeths.co.uk info@macbeths.co.uk 0118 916 5480

Insuranceage top 100 independent brokers
OUTSTANDING TO WORK FOR 2024
Chartered Insurance Brokers

Authorised and regulated by the Financial Conduct Authority (FCA) under reference 305922.
M S Macbeth Ltd. Registered office: 2nd Floor, Nucleus House, 2 Lower Mortlake Road,
Richmond TW9 2JA. Registered in England and Wales. Reg no. 03408293.

5