Business attitudes to cyber security

Managing the risks that come with the digital age

February 2024

Introduction

As digital acceleration gathers pace, so do the risks posed by cyber crime. Our survey of UK business leaders in partnership with YouGov* reveals the risks that leaders are most worried about and what actions they take when it comes to cyber security.

Since last year's results, 17 percentage points more businesses now see cyber security as a major risk to their organisations. Large corporates with sophisticated tech stacks rate it as the number-one risk (46%), while mid-market business leaders saw it as their second-largest risk (38%) after skilled workforce shortages.

However, small businesses ranked cyber security sixth (17%) compared to other major threats such as business interruption (31%) or negative online reviews (20%).

With an over-reliance on multiple third-party services, many small businesses could be underestimating the likelihood and impact of a breach.

Worries over cyber attacks have risen from 40% to 57% since 2020. What's interesting is that 49% of businesses rate themselves as resilient to all identified risks and just 10% rate themselves as not resilient.

While small businesses saw fewer risks as major when it came to resilience, only 43% of them felt resilient compared to 59% of corporates.

*YouGov Survey, 1,218 senior business leaders surveyed between 15 September to 8 October 2023.

Most common cyber attack methods

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 publish.

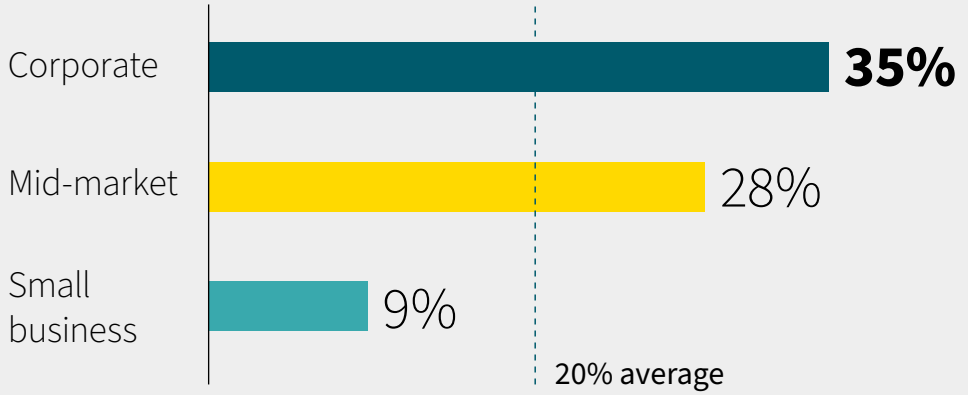
Social engineering scams
Deceptive techniques used to manipulate individuals into divulging confidential information or making a payment to fraudsters, causing data breaches and financial loss.

What's the true impact of cyber crime?

Our research reveals that one in five UK businesses have been a victim of a cyber attack in the last 12 months. This rises to as high as one in three when looking at corporates alone – whose size could not only make them attractive targets but also increase the complexity of protecting themselves against attacks.

It's important to note that small businesses are not immune; cyber attacks happen indiscriminately.

Businesses who admitted to being a victim of a cyber attack or online fraud in the last year



What do cyber attacks cost?

For more than one in four businesses (26%) the cost of cyber attacks on UK businesses was over £10,000. An attack can sometime cost millions, even for moderate sized businesses and our own Aviva claims data shows that 10% of the Cyber claims we received in 2023 were valued in excess of £50,000.*

It's not just the financial cost. Almost a third (32%) of businesses that experienced an attack in the last year suffered operational disruption, with one in five (21%) hit by a loss of data and being locked out of systems. Larger organisations reported double the impact on employees' stress levels.

If customer data is involved, there may be GDPR notifications and issues to resolve – the use of a third-party system doesn't remove that regulatory obligation from the business.

After an attack, companies are keen to prevent a future incident: 68% have already taken the actions they need to improve security, and 29% are still implementing changes.

*Taken from 2023 Aviva commercial claims data

Are businesses taking the right steps to protect themselves?

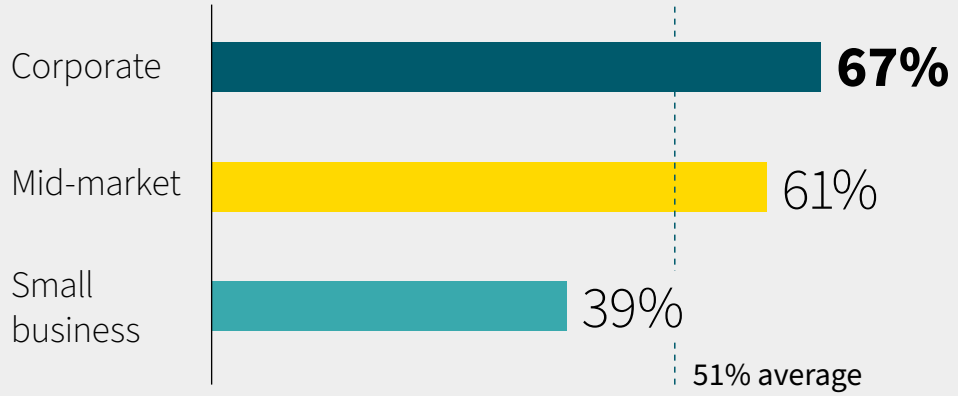
Leaders are quite confident in their organisation's ability to stop an attack – more than half (56%) believe their cyber security protections will suffice. For large corporates, who are likely to have dedicated security teams, this confidence rises to 64% of businesses.

However, that confidence lessens in the event of an attack. Just 51% of all businesses felt sure about their next course of action. Corporates are more confident in their ability to react, but just two in five (39%) small business owners felt they would choose the right action if their systems were breached.

In the face of a potentially business-disrupting event, a fast response is vital – and businesses often need to engage expertise across several disciplines at pace, from data recovery and IT forensics to legal advice and PR/ reputational management.

> Just 51% of all businesses felt sure about their next course of action.

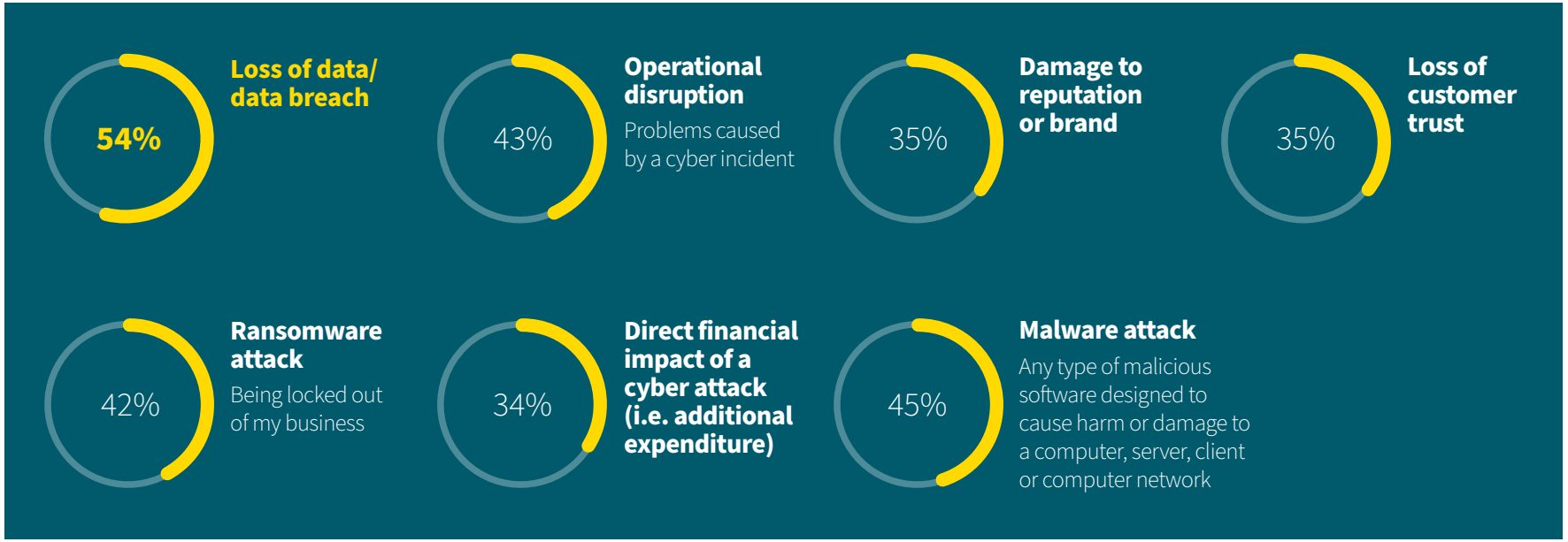
Businesses who are confident they know what to do in the event of a cyber attack



What worries businesses the most about an attack?

Loss of data or a data breach is the number-one concern for most businesses (54%), regardless of their size. While data can have a direct impact on the day-to-day running of a business, there are also stiff 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. With large interconnected systems, modern businesses are increasingly vulnerable to attacks – the loss of any system could have wider impacts across the business or for customers.

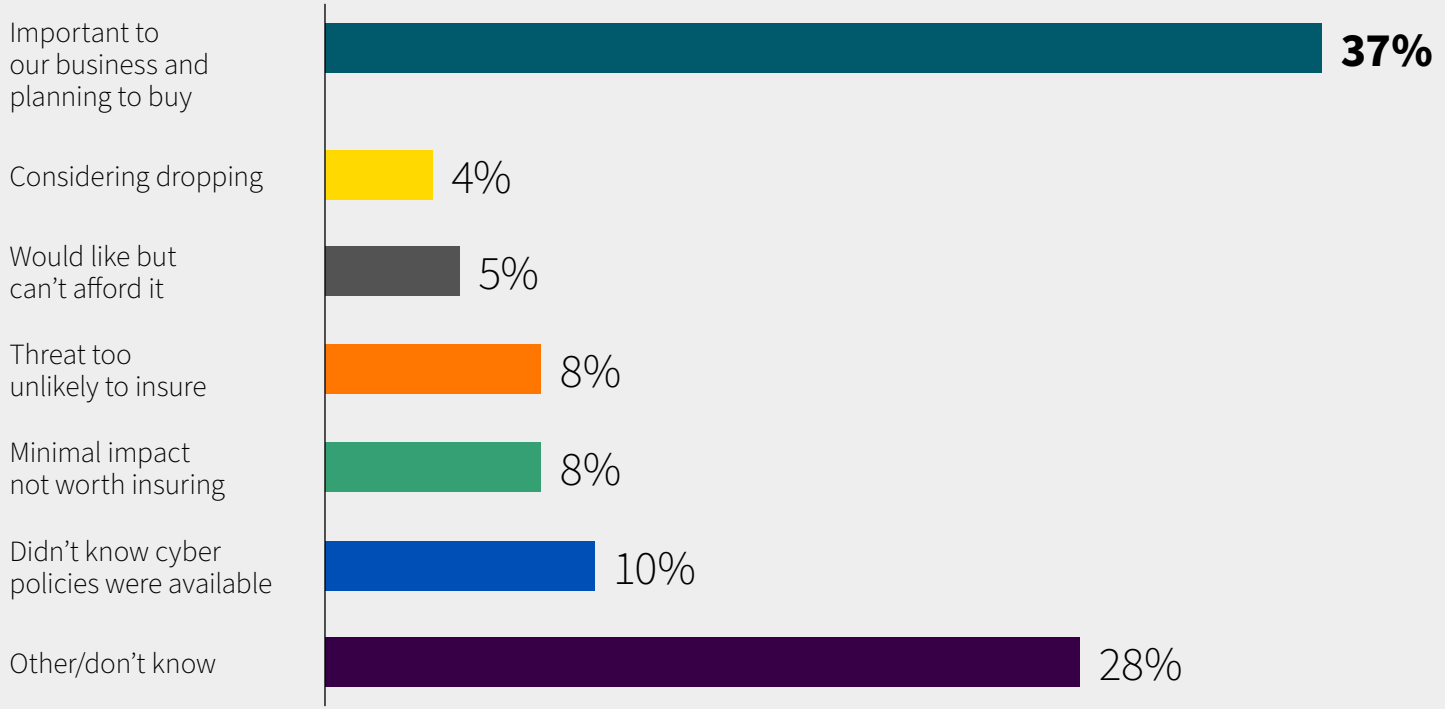


Adding layers of protection against cyber risks

Cyber security insurance is a growing market, but just 37% of businesses see having cyber insurance as important to them or are planning to buy it. Small businesses are generally less aware that these policies exist – and probably don't know that these policies offer access to expertise and support during and after an attack, as well as financial compensation.

We often find that the number of companies that believe they have cyber cover in place can be notably higher than the number that actually do – a worrying pattern that suggests many businesses believe they are protected when that may not be the case.

Business responses to getting cyber insurance

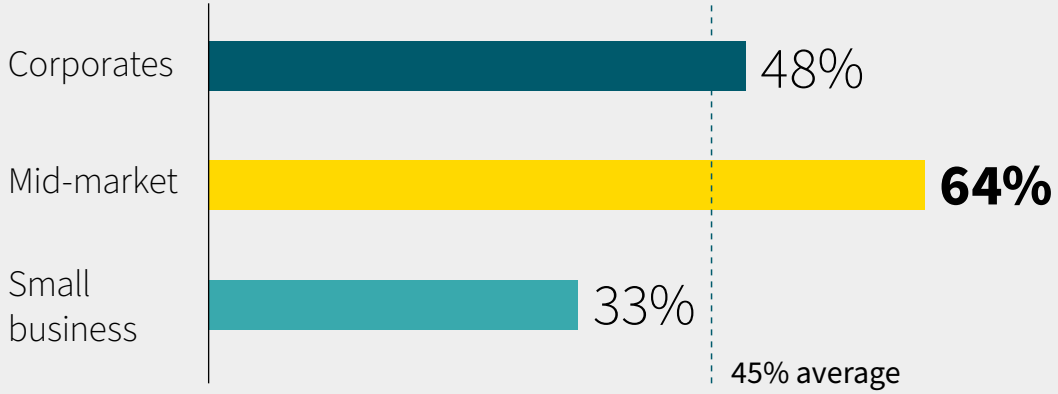


Of businesses with online fraud and cyber attack policies, just 45% have reviewed their cover over the last year.

At one end, time-pressed small businesses are the least likely to check their cover, while close to two-thirds of mid-market businesses have reviewed or will be reviewing their policy.

The good news is that 56% of businesses are looking to maintain their level of insurance. Despite macroeconomic headwinds, almost 1 in 10 businesses (9%) want to increase their cover to account for growth and inflation as well as rising concern about cyber disruption. Against this background, only 4% are looking to reduce cover while 7% are consulting their brokers to better understand their needs.

Businesses which have reviewed their insurance cover for cyber/ online fraud in the last 12 months or plan to before the end of the calendar/financial year



Preparing for the future

Without a doubt, continued digitisation is creating opportunities for growth as well as increasing risks.

More than half (56%) of leaders are worried about new and changing technology – businesses are having to look at how new technology will change their business models and, at the same time, make sure their cyber security is protected.

"Our research shows that businesses are more likely to put in place sufficient cyber cover after having experienced an attack, rather than before," says Stephen Ridley, Head of Cyber. "However, cyber insurance doesn't just provide cover for the costs incurred from an attack but provides access to experts to respond immediately to the incident. We are also working to equip brokers with a deeper understanding of cyber risks and insurance mitigations, as we know that they play a vital role in educating and advising their customers."

In recognising that small businesses, especially micro-SMEs, need cover tailored to their needs and budgets, Aviva has launched a new cyber insurance policy, Cyber Respond, which focuses on rapid breach response services and starts from as little as £50 (plus Insurance Premium Tax). And for larger businesses, there's Cyber Complete, offering a comprehensive breadth of covers designed to meet the protection needs of large SMEs and mid-market organisations. Aviva is also supporting brokers to help clients improve their levels of cyber security to help mitigate the risks they face.

> Whatever their size or sector, businesses are at risk of a cyber attack. One of the key steps in protecting themselves from this emerging threat is to speak to their broker – they can work with businesses to support their cyber security, including addressing their cyber insurance needs."
>
> **Stephen Ridley**

Thank you

For further support and guidance on cyber and data management risks, visit the **Aviva Risk Management Solutions site**