cfc

CFC Signals: SME Insights

The Cyber Insurance Disconnect

2026-2027

Contents



Introduction

03 Cyber awareness has grown – understanding hasn't

The disconnect

07 Cyber awareness is no longer the challenge

10 Many SMEs underestimate the threats they face

The emerging disconnect

16 AI risk is outpacing cyber insurance adoption

The connection

19 SMEs feel more confident with cyber insurance

22 The future cyber conversation starts here

Cyber awareness has grown – understanding hasn't

For years, the cyber industry's challenge has been helping businesses recognize that cyber risk is real. That challenge has largely been overcome. As cyber attacks become more frequent and businesses grow more reliant on digital systems, cyber risk has become part of everyday business reality.

This marks a turning point for brokers. The challenge is now helping businesses understand where they're exposed and how they can respond with confidence.



Nearly 1 in 2 SMEs rank cyber as their biggest business risk – yet many still remain unprotected against it

In this landscape, cyber can no longer be viewed as an emerging risk. It's a core business concern, sitting alongside – and often overtaking – more established exposures such as property, crime and professional liability. So why does uptake of cyber insurance remain low, particularly among small and medium-sized enterprises (SMEs)?

Our SME survey reveals key gaps in how SMEs perceive cyber risk and the role cyber insurance can play in protecting them. While many rank cyber as their biggest business risk, fewer realize:

- The cyber threats most likely to impact their business
- What cyber insurance actually covers, and the support available
- How AI is changing their cyber exposure
- What good cyber preparedness really looks like

This is the cyber insurance disconnect.

For brokers, the opportunity is to help clients understand how cyber risk applies to their business, guiding them to the right insurance – and giving them confidence they're protected.

About the survey

We commissioned independent research among 2,000+ decision-makers across the UK, US, Canada and Australia.

The survey included business owners, directors, IT and cyber security leaders, and finance decision-makers from organizations with annual revenue equivalent to £25 million, spanning 10 industry sectors.

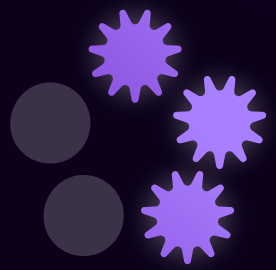
All statistics represent the combined results of all surveyed markets (UK, US, Canada and Australia) unless a specific region is noted.

SME survey: Key findings at a glance

#1

Cyber is ranked the top business risk

Far more likely to be cited than property, crime and professional liability



Nearly

3 in 5

have experienced a cyber event in the last three years

3 in 4

don't realize cyber insurance covers human-error related incidents

2 in 3

don't realize comprehensive cyber insurance includes proactive cyber security protection and legal support

Only 30%

identify phishing and social engineering as a major threat despite them being among our most common claim types

SME survey: Key findings at a glance

94%

with cyber insurance say they feel confident managing cyber risk

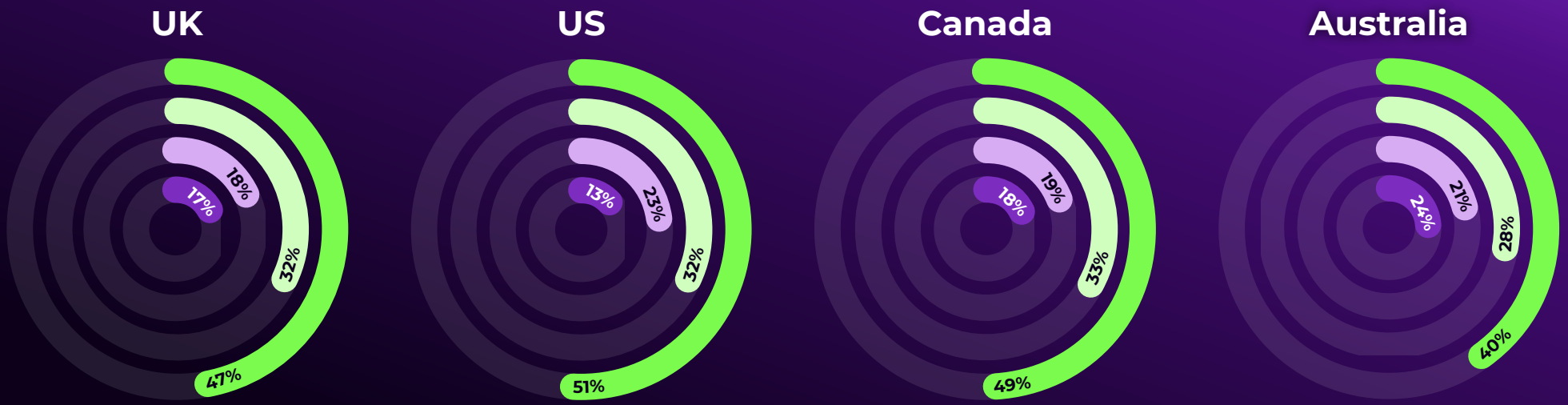
68%

expect AI to increase organizational risk over the next two to three years


The
disconnect

Cyber awareness is no longer the challenge

What SMEs view as their biggest business risks



- Cyber attack or data breach
- Professional errors
- Loss of staff
- Fire or property damage

SMEs see cyber attacks as their **top business risk**

Cyber awareness is no longer the challenge

Our research reveals cyber is now cited as the number one business risk, outranking many traditional concerns including fire and property damage, loss of staff and professional errors.

This is a fundamental shift in how SMEs view risk. While events such as fires can be devastating, for most organizations they're relatively infrequent. Cyber risk, by contrast, is something SMEs face every single day, with a growing range of threats targeting the very digital systems they depend upon to communicate, trade, process payments and deliver services to customers.

SMEs are already seeing the impact. Across all four countries surveyed, more than half reported experiencing a cyber event within the past three years. The findings challenge the perception that smaller businesses are unlikely to be targeted and underline just how common cyber incidents have become.

The central question

If cyber is recognized as the biggest business risk, why do so many SMEs continue to retain that risk themselves rather than transfer it through insurance?

What does this mean for brokers?

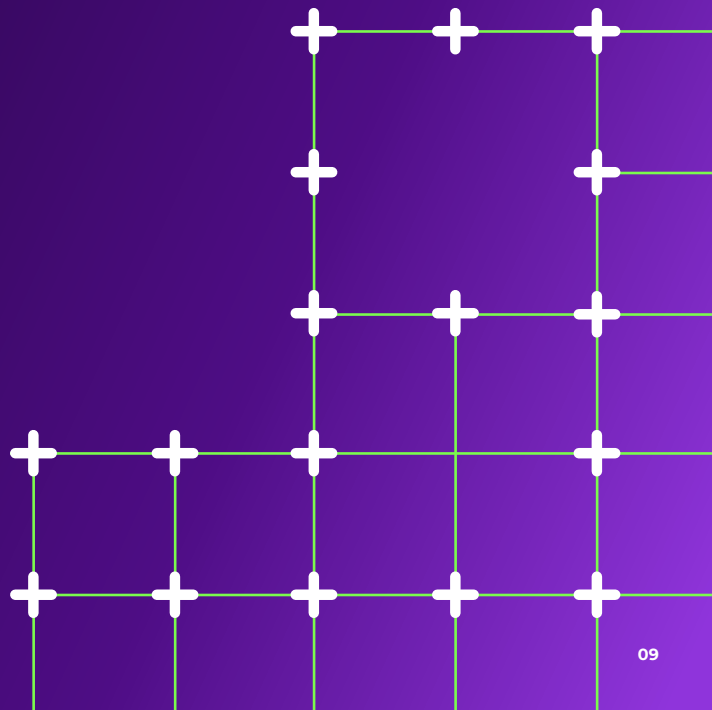
SMEs are already telling us they recognize cyber as a serious business risk. As threat actors scale their operations and target supply chains, the client conversation is shifting from awareness of the threat to understanding exposure, impact and resilience.

The opportunity is to help clients understand:

- Where and why their business is exposed
- What the consequences could be
- How cyber insurance is vital in preparing for, responding to and recovering from incidents

Nearly 3 in 5 SMEs have experienced a cyber event in the last three years

UK: Nearly 3 in 5 | US: 1 in 2 | Canada: 1 in 2 | Australia 7 in 10



Many SMEs underestimate the threats they face

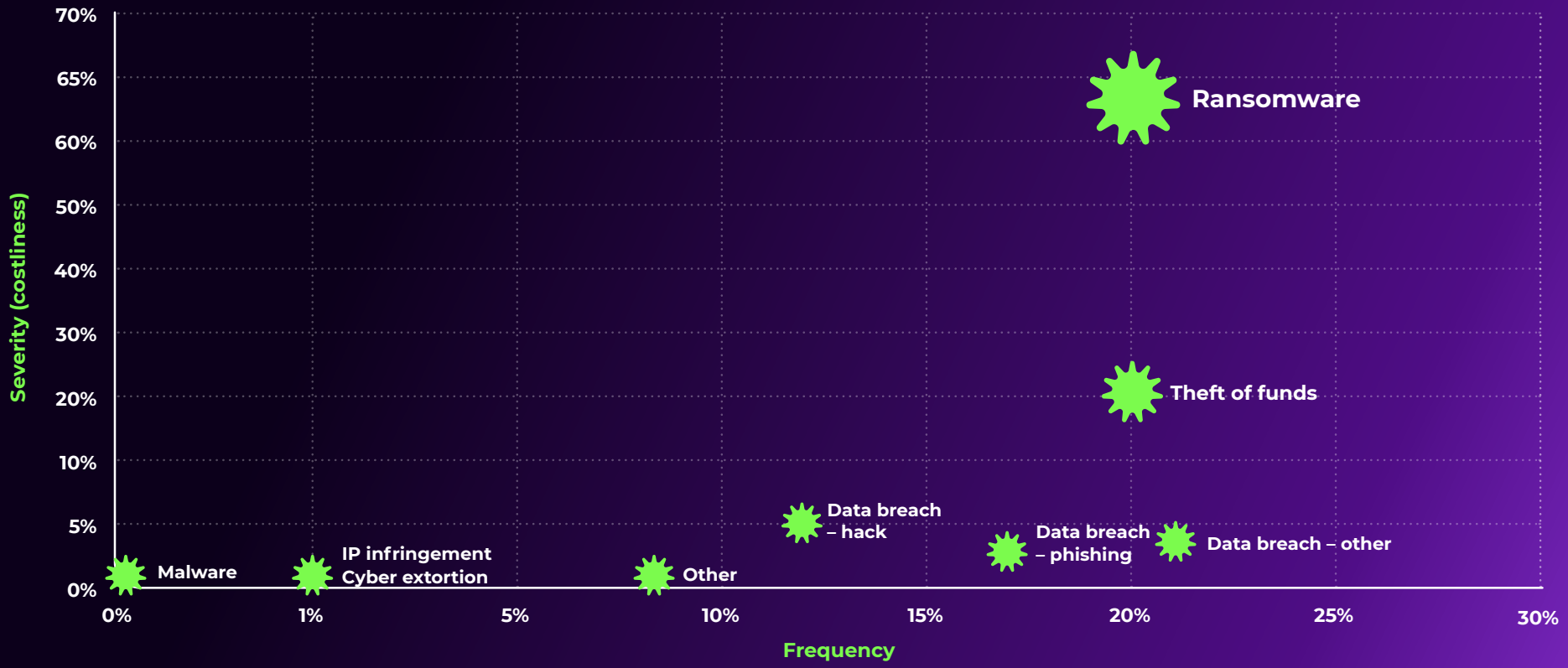
Only 30% identify phishing and social engineering as a major threat	**Despite theft of funds and phishing being among the most common cyber claims***
Only 30% identify ransomware as a major threat	**Despite ransomware accounting for the majority of cyber claims costs at 64%***
Only 28% identify human error as a major threat	**Despite human error contributing to 75% of cyber claims***

Cyber risk is named the top business risk, but many
SMEs don't know where they're vulnerable

CFC cyber claims data from January – December 2025

Many SMEs underestimate the threats they face

CFC cyber claims impacting SME businesses*



CFC cyber claims data from January – December 2025

Many SMEs underestimate the threats they face

The findings suggest many SMEs still think about cyber risk in broad terms, rather than focusing on the specific threats they're most likely to face. SMEs don't need to understand every danger out there. But if they underestimate the threats most likely to affect them, how can they prioritize the protection that's needed?

Today's cyber threats often hide in everyday business activities. A seemingly legitimate supplier email requesting updated bank details can result in an invoice being paid into a fraudulent account, while a single click on a phishing link can give a threat actor access to company systems. With AI making scams more convincing, easier to scale and lowering the barrier to entry for cybercriminals, any business with employees and computers is exposed.

Yet despite the potential impact of these incidents, our research shows there's often a mindset of, "I know it's a risk, but it's probably not my risk."

What does this mean for brokers?

Cyber conversations are most effective when they start with the risks facing the business, not the insurance solution. Before discussing coverage, clients first need to understand:

- The threats most likely to affect their organization and industry
- What those threats look like in practice
- How they can disrupt day-to-day operations
- The financial and operational consequences of an attack



Threat actors target businesses that are vulnerable, not valuable, which makes SMEs attractive targets. Whether caught up in larger attacks or used as a route into bigger organizations, many of these businesses lack the dedicated security resources to defend against today's cyber threats – leaving them particularly exposed.

Lindsey Maher, Head of Global Cyber Development, CFC

Few SMEs understand what cyber insurance really offers*



This shows that **many SMEs are unaware** of how cyber insurance responds and provides this vital support

*Those who are aware of cyber insurance

Few SMEs understand what cyber insurance really offers

Perhaps the most striking insight from the research is not what SMEs think about cyber risk, but what they think cyber insurance includes. They recognize cyber insurance by name – but when it comes to what's actually on offer, there are big gaps in understanding.

Many SMEs don't recognize the key features of cyber insurance, including legal and regulatory support, proactive cyber security services that help prevent incidents, and expert incident response to minimize their impact. That's despite these being core components of comprehensive cyber insurance.

In the same vein, while human error contributed to 75% of CFC cyber claims in 2025, nearly three in four SMEs believe these incidents aren't covered by cyber insurance. There's also a widespread misconception that cyber insurance claims won't be paid. Yet cyber insurance is designed to respond to a broad range of incidents, with 99.4% of CFC cyber claims accepted*.

This is a key part of the cyber insurance disconnect. Many SMEs underestimate both the breadth of cover and the support it provides beyond paying out claims. In reality, cyber insurance is a broader resilience solution, helping businesses prepare for, respond to and recover from cyber incidents.

What does this mean for brokers?

The cyber insurance industry has spent years helping SMEs understand why cyber risk matters. The next phase of market growth will come from helping SMEs understand that cyber insurance can offer more than financial protection alone.

Rather than leading with policy wordings, limits and premiums, brokers should highlight the services included to help clients understand:

- How cyber insurance responds to common causes of cyber incidents, including human error
- What proactive cyber security services are included and how they work to reduce risk and prevent attacks
- When they can access specialist support – not only when they suffer a incident but also throughout the policy period
- How cyber insurance provides expertise, protection and recovery support, not just a claims payment

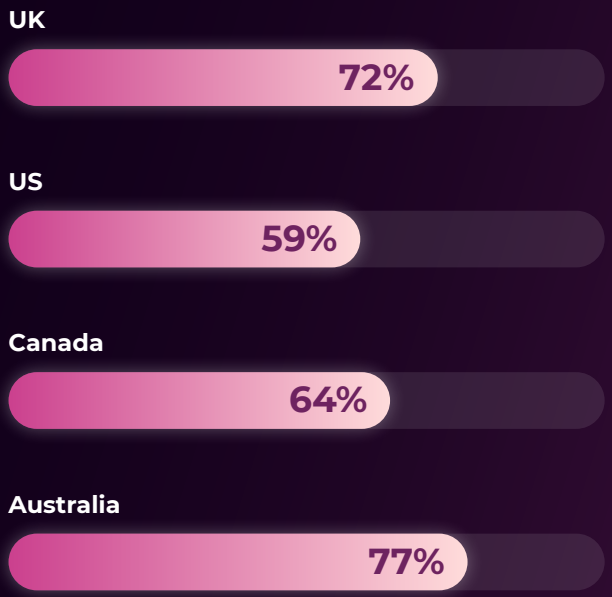
By focusing on services rather than policy clauses, brokers can help bridge the gap between what SMEs think cyber insurance offers, and the broad protection actually available through a modern cyber policy.

**CFC cyber claims data March 2025 – March 2026*

The emerging disconnect

AI risk is outpacing cyber insurance adoption

68% of SMEs expect AI to increase organizational risk over the next 2 to 3 years



AI is becoming a mainstream business risk

Businesses increasingly view AI as a force driving cyber risk. Our research shows SMEs are 11 times more likely to expect their AI exposure to increase than decrease over the next two years.

A key factor is the pace of AI adoption. Businesses are integrating AI-powered tools across their operations to remain competitive. However, many are still building the understanding and processes needed to manage the associated risks. The result is a growing disconnect between AI integration and AI readiness.

11x
more likely

AI risk is outpacing cyber insurance adoption

AI is a catalyst for more efficient cyber attacks

AI is reshaping the cyber threat landscape. While it's becoming an important part of security – with AI able to help prevent attacks, identify threats earlier and accelerate recovery after an incident – AI is also being harnessed by threat actors for malicious activities.

However, rather than introducing entirely new forms of cyber risk, it's important to note AI more often increases the speed, scale and sophistication of existing attacks. In this way, AI acts as a catalyst to make attacks more realistic and harder for businesses to identify, while lowering the barrier to entry for prospective threat actors.

Phishing attacks

AI tools can create highly-realistic deepfakes and hyper-personalized emails, making phishing campaigns both cheaper to produce and harder to spot.

Ransomware

By speeding up reconnaissance and analyzing stolen data, threat actors are using AI to scale attacks and make ransomware campaigns more effective.

Vulnerability discovery

Threat actors are using AI to find weaknesses in systems and applications, so they can launch a greater volume of attacks in less time.

What does this mean for brokers?

As AI adoption accelerates, many businesses are beginning to ask a new question: what does this mean for our insurance cover?

While there's widespread recognition that AI is influencing cyber risk, many SMEs aren't certain their existing policies will respond to AI-related exposures. As a result, they're looking for greater clarity and reassurance around how their coverage applies.

For brokers, this creates an opportunity to demonstrate how cyber insurance is keeping pace with AI-related risks.

Affirmative AI coverage provides greater certainty around how a policy should respond*, giving clients confidence that their insurance is keeping pace with the technology they're adopting.

*Cover and services are subject to the applicable policy terms, conditions, limits and exclusions.

The connection

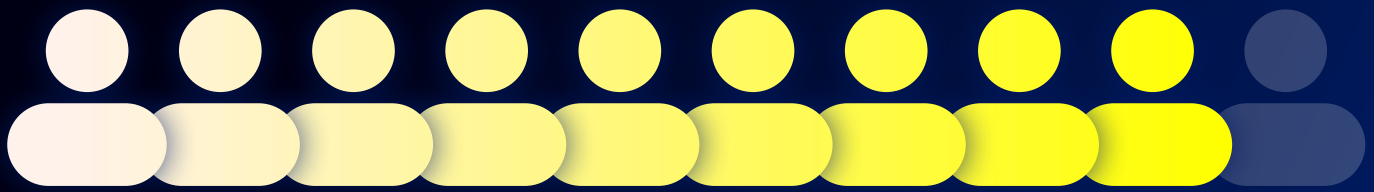
SMEs feel more confident with cyber insurance

SMEs with cyber insurance:

94%

are confident they can manage cyber risk (vs. 61% without cyber insurance)

Are **23x** more likely to have a formal cyber strategy



9 in 10

have business continuity plans in place

SMEs feel more confident with cyber insurance

Throughout this report we've explored a series of disconnects. But the research also reveals a notable connection: SMEs with cyber insurance consistently report higher confidence levels, stronger planning and greater preparedness than those without it.

This suggests cyber insurance may play a much wider role than simply transferring risk. The findings point to a strong correlation between having cyber insurance and taking a more structured approach to preparing for cyber events, with insured SMEs reporting a greater focus on cyber security, incident response and recovery planning.

Rather than choosing between cyber security and insurance, the findings suggest SMEs can view them as complementary parts of the same strategy – reducing the likelihood and impact of an incident, while providing specialist support when something does go wrong.



The SMEs that appear most prepared for cyber risk are often the ones with cyber insurance, yet uptake remains relatively low. Right now, the market has a huge opportunity to close this gap.

Scott Bailey, Head of Global Cyber Underwriting, CFC

What does this mean for brokers?

Cyber insurance is often viewed as a safety net for when something goes wrong. Yet the research shows many SMEs with cyber insurance also report greater confidence in their ability to manage cyber risk and respond to incidents.

This creates an opportunity to look beyond the policy itself. On top of financial protection, cyber insurance can help businesses become better risks, while providing access to specialist cyber security expertise and proactive support – to help keep them ahead of emerging threats.

So why do many SMEs go without cyber insurance?

Businesses with cyber insurance are more confident in their ability to manage cyber risk and are more prepared to do so. Yet despite this connection, many SMEs navigate today's escalating threat landscape without dedicated cyber cover in place.

Key takeaways

- **Cyber insurance builds confidence through capability:** Insured SMEs feel more capable of handling an incident – and that confidence can support a more proactive approach to planning, processes and recovery.
- **Cyber insurance supports resilience, not just protection:** SMEs with cyber insurance report stronger preparedness, including more robust planning, continuity measures and recovery processes.
- **Cyber insurance is more than risk transfer:** It provides access to cyber security services, specialist incident response support, expert partners and claims expertise when SMEs need it most.

What does this mean for brokers?

The cyber insurance disconnect is really an education gap. Most SMEs fail to see how cyber insurance supports a wider resilience strategy, and why they need insurance in the first place.

Today, cyber insurance should be seen in the same way as property insurance. Businesses have locks on their doors and fire alarms in their buildings, but they still buy property insurance in case those measures fail. Cyber risk is no different. Investing in cyber security is essential, but even strong controls can be bypassed and human error exploited. That's where cyber insurance comes in.



Perhaps the biggest takeaway from this research is that cyber awareness is no longer the barrier it once was. SMEs are paying attention. They're concerned about cyber risk and they're ready to have the conversation. The opportunity now is to make that conversation more relevant, practical and meaningful. No group is better positioned to do that than brokers.

James Burns, Global Head of Cyber, CFC

The future cyber conversation starts here

Evidence of today's escalating threats is everywhere. Three in five SMEs have experienced a cyber event in the last three years, and nearly one in two rank cyber as their biggest risk.

Cyber coverage is now a need-to-have. And the encouraging news is SMEs are ready for the discussion. Yet while awareness of cyber risk continues to grow, many businesses still don't fully understand what cyber insurance actually does. This research highlights an opportunity to show clients how cyber insurance responds to incidents and the support available before, during and after an event.

Today's brokers are uniquely positioned to help close the cyber insurance disconnect, turning cyber awareness into meaningful conversations about exposure, resilience and protection – and increasing cyber insurance penetration among SMEs.



Ready to close the cyber insurance disconnect?

Find simple questions to help clients understand where they are exposed and how cyber insurance bridges the gap.

Explore conversation starters

Want to find out more or get a cyber quote? Get in touch with our team at **cyber@cfc.com**.

Methodology

This report is based on independent research conducted in June 2026 by Censuswide on behalf of CFC among 2,004 SME decision-makers involved in cyber security purchasing decisions across the UK, US, Canada and Australia (501, 500, 501 and 502 respondents respectively). Respondents represented organizations with up to £25 million in annual revenue (USD $33.75m, CAD $46.5m and AUD $47m) and included Directors, Company Owners, Company Founders, IT and Cybersecurity Decision-Makers, and Finance Decision-Makers. The research included an equal representation of organizations across the following industries: Construction, Education, Financial Services, Healthcare, Manufacturing, Professional Services, Public Entities, Retail, Technology, and Transport & Logistics.

Censuswide is a member of the Market Research Society (MRS) and the British Polling Council (BPC), and a signatory of the Global Data Quality Pledge. We adhere to the MRS Code of Conduct and ESOMAR principles.

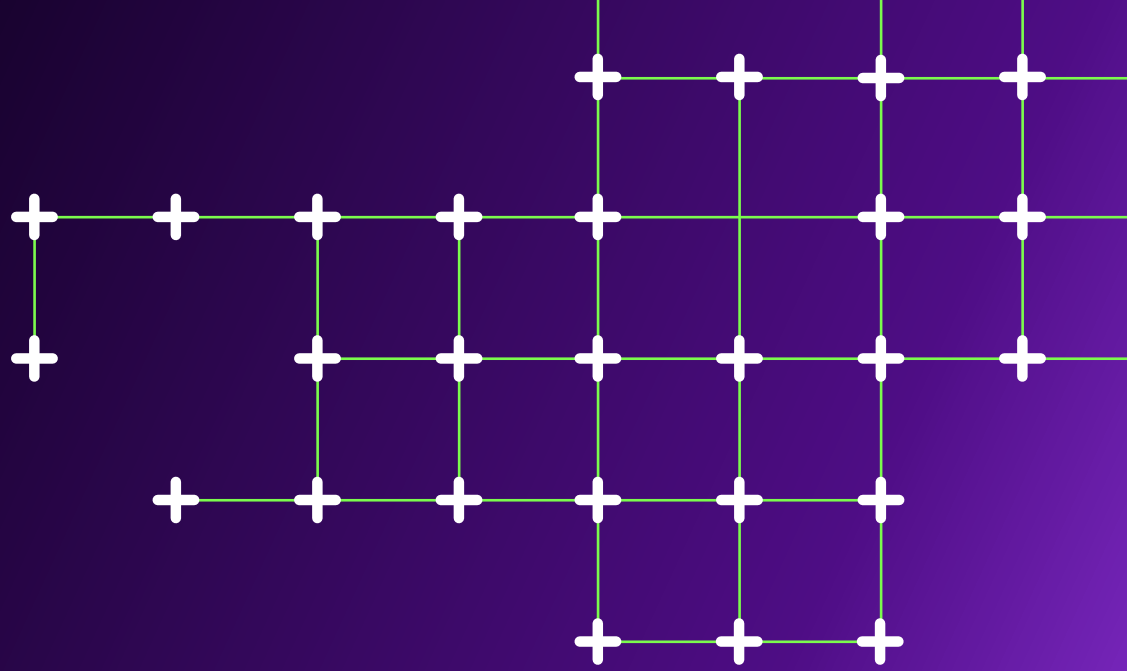
Purpose and disclaimer

This report is intended to help brokers and businesses better understand SME attitudes towards cyber risk, cyber insurance, resilience and emerging threats, and to support more informed conversations about cyber protection and preparedness.

The findings, statistics and insights presented in this report reflect the views, experiences and perceptions of survey respondents at the time the research was conducted. Where referenced, CFC claims data has been included to provide additional context and illustrate trends observed within CFC's cyber portfolio. Survey findings and claims data should be considered in context and do not guarantee future outcomes or experiences. They are intended to provide general market insight and information for the purpose described above and should not be interpreted or relied on as providing any legal, regulatory, insurance, risk management, or other advice. Individual business circumstances, risk exposures and insurance requirements will vary – please seek independent professional advice if you are unsure.

Note on confidence and preparedness

The confidence, awareness and preparedness measures referenced throughout this report are based on respondents' self-assessment. While many SMEs report confidence in their ability to manage cyber risk, these findings should not be viewed as evidence of actual preparedness, resilience or organizational security maturity. One of the key themes emerging from the research is the gap that can exist between perceived understanding and awareness of specific cyber threats, insurance protections and resilience measures. The findings are intended to support informed discussion and should be considered alongside an organization's individual circumstances, risk profile and protection needs.



About CFC cyber

CFC has been providing market-leading cyber insurance for over 25 years. Trusted by more than 100,000 customers globally, we strive to offer comprehensive cyber cover to every business.

Our offering includes proactive cyber security services as standard, helping businesses prevent cyber attacks before they happen. And if an incident does occur, our industry-leading in-house incident response and global cyber claims teams are there to get businesses back online, fast. Learn more at **cfc.com** and **LinkedIn**.

CFC Underwriting Limited is authorized and regulated by the Financial Conduct Authority. For more information on the Financial Conduct Authority, visit fca.org.uk. CFC Underwriting Limited is registered in England and Wales with company registration number 03302887.
Registered office: 8 Bishopsgate, London, EC2N 4BQ © 2026 CFC Underwriting Limited. All rights reserved.

Last updated 1026