Cracking the Cyber Market Code

Insight pack

Uncovering the cyber cover and service priorities for brokers and SMEs

MARKEL

Contents of this report

3.
Introduction to this report

4.
SME and insurance broker research methodology

5.
How SMEs view cyber insurance

6.
Understanding SME buying preferences in the cyber market



7.
How brokers view the cyber insurance landscape

8.
Brokers' perspectives on comparing cyber cover and meeting client needs

10.
Understanding broker pain points in the cyber sales journey

Introduction to this report

While awareness of digital threats amongst UK businesses is at an all-time high, our research indicates a significant disconnect between the perceived and actual value of cyber insurance cover. Policyholders and brokers alike continue to deal with unclear wordings and inconsistent terminology, all against the background of an assumed lack of relevance to the day-to-day operations of SME businesses.

This report aims to understand that gap. By capturing the views of UK SMEs and leading brokers, including members and the chair of the BIBA Cyber Committee, we have identified many of the issues that exist in the market today, including friction points in the broker/ customer sales journey.

Our goal at Markel is to move cyber insurance from a transactional “grudge purchase” to an essential and valued form of insurance protection. Seeking the input of customers is essential to achieving this objective and our Cracking the Cyber-Market Code report reveals details of the feedback and findings from this process.





SME and insurance broker research methodology

Our findings are the result of an extensive research programme conducted in 2025, combining broad quantitative data with deep qualitative insights, ensuring that the strategic recommendations provided represent the day-to-day realities of both policyholders and their advisors.

We captured the views of over 1,500 UK SMEs, businesses of various sizes and sectors. This allowed us to identify the specific triggers, barriers and perceptions that define the current SME appetite, or lack thereof, for cyber protection. Looking at organisations with turnover of both below and above £10 million, helped us gain an understanding of how business maturity impacts cybersecurity confidence and insurance uptake.

In-depth qualitative research was undertaken with 16 insurance brokers. The group deliberately included a mix of account executives advising smaller SMEs on a daily basis and senior specialist brokers handling more complex digital risks. Importantly, our research involved multiple members of the BIBA Cyber Committee, including its chair. This committee brings together the UK's leading experts to help shape and promote cyber insurance, and their participation provided our research with a unique level of strategic depth and insight.

How SMEs view cyber insurance

For UK SMEs, digital risks are a daily reality. Our data shows that 53% of SMEs now agree that cybercrime and data breaches are among the most important challenges facing their business over the next few years.

Of the sample, 44% did not have cyber insurance cover. The main reason given for this was low perceived risk, with 39% of SMEs believing they are simply too small to be a target or that their specific business activity carries low exposure. This view is often affected by "headline bias", where business owners see high-profile attacks against major corporations like M&S or Co-op in the media and mistakenly conclude that hackers only go after larger organisations.

As one specialist broker noted:

"The level of cyberattacks doesn't correlate at all to the turnover of the company and some stats show that more than 3/4 of attacks are happening to SME businesses. Even though that's not what's been seen on the media. Obviously, you get all the big sexy stuff on BBC News, but the reality is that it is the lower-hanging fruit that is most impacted."

Overall, the top three reasons stated for not having cyber insurance were:

39% Risk to business is low

25% Too expensive

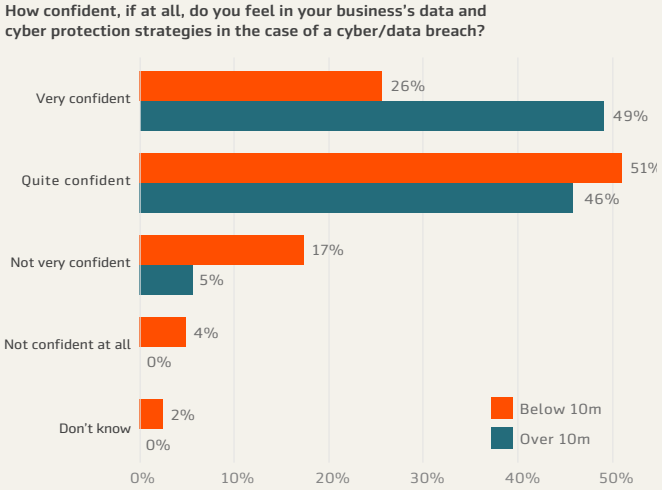
24% I don't know enough about it and what it offers

This misplaced optimism can be down to a lack of technical understanding with owners not fully grasping the extent of their existing digital safeguarding or why they would be targeted.

For instance, 13% of businesses assume their outsourced IT provider handles all aspects of cyber risk, failing to realise that IT teams focus on prevention, while insurance handles the consequences of an incident. Furthermore, 11% of SMEs mistakenly believe they are already covered by other insurance, leaving the business dangerously exposed.

The research also identified a significant "confidence gap" within the SME community. Only 26% of smaller businesses report feeling "very confident" in their data and cyber protection strategies. Larger companies are more confident, at 49%.

This lack of certainty suggests that while business owners know they are at risk, they feel under-equipped to address it.



This is further evidenced by the fact that 37% of insured SMEs have made a claim, compared to just 7% of those without cover. This contrast implies that many businesses will only look to actively purchase cyber protection after an incident or close call.

Understanding SME buying preferences in the cyber market

Our research reveals that SME purchasing behaviour in the cyber space is changing from searching for a product to searching for answers to problems.

Small business owners will not typically start by searching for “cyber insurance”. Instead, they use search engines to find answers and solutions for crises or governance questions, such as “What do I do if my client data gets hacked?” or “Is cyber insurance really worth it for a business like mine?”.

This highlights the need for the insurance sector to provide helpful, jargon-free content that answers real-world questions in everyday language.

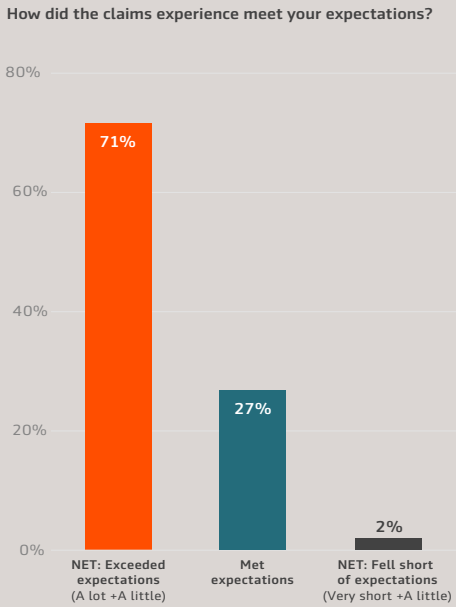
When evaluating the attractiveness of a policy, 39% of the SME respondents purchase the cover to guard against financial loss but the proactive services that help to prevent a breach from occurring in the first place are an important consideration.

Tools like vulnerability benchmarks, posture assessments, and risk-calculators, which make digital risk feel measurable and relevant upfront, are highly valued. Once a policy is bound, the ongoing support offered is now rated almost as highly as the claims handling itself. Training, live monitoring, and real-time threat alerts provide a tangible “return on investment” that helps business owners justify the annual premium cost.



Cyber claims perception

While many SMEs initially view cyber insurance as a “grudge purchase”, those who have actually claimed their policy report an overwhelmingly positive experience. 71% of SMEs who made a cyber claim stated the experience exceeded their expectations.



The insurance sector has the opportunity to further improve on this by better serving these clients through a more structured cyber protection journey including pre-bind scanning, day one support, active monitoring and a clear response promise.

These improvements will help to move the discussion from premium costs toward business continuity and resilience, providing the greater motivation to purchase that first-time buyers need to protect themselves.

After all, as one broker respondent pointed out:

“Cyber feels important, but it’s hard to get clients to listen when they’re focused on price.”

How brokers view the cyber insurance landscape

In a market that is often seen as overcrowded and technically complicated, brokers are seeking a combination of the speed and simplicity of service required for SME placements without sacrificing the technical depth needed for complex risks.

“There’s too much jargon and not enough clarity, it makes clients switch off,” said one broker respondent.

A “frictionless” client journey is an important requirement for brokers. In fact, 84% of those questioned said that clients care most about the right level of cover at the right price, but a significant 69% say ease of use is now a critical buying factor.

Beyond the transaction, brokers value insurers who act as genuine partners in client education. They need help to close the confidence gap which can be a challenge for some.

“I’m advising my clients why they need something but I’m not technical enough to know what the all the answers are,” said one respondent broker.

“There’s too much jargon and not enough clarity, it makes clients switch off,” said one broker respondent.



Broker perspectives on comparing cyber cover and meeting client needs

The lack of wording and cover standardisation across the UK cyber insurance market is creating a challenge for brokers.

Our research found that 100% of the brokers we spoke to, regardless of their experience level, reported confusion when trying to compare cover and limitations across different providers.

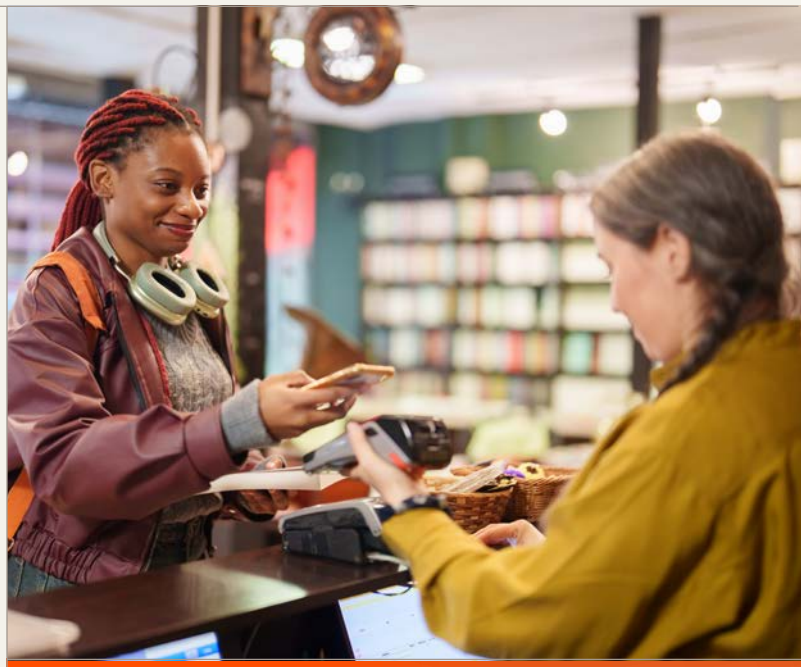
This is primarily driven by inconsistent terminology. When one provider uses the term “social engineering” and another uses “eCrime” to describe similar risks, brokers are forced to spend excessive time interpreting wordings. This not only slows down the comparison process but significantly increases the broker’s Errors & Omissions (E&O) exposure if they mistakenly assume a risk is included or excluded based on ambiguous language.

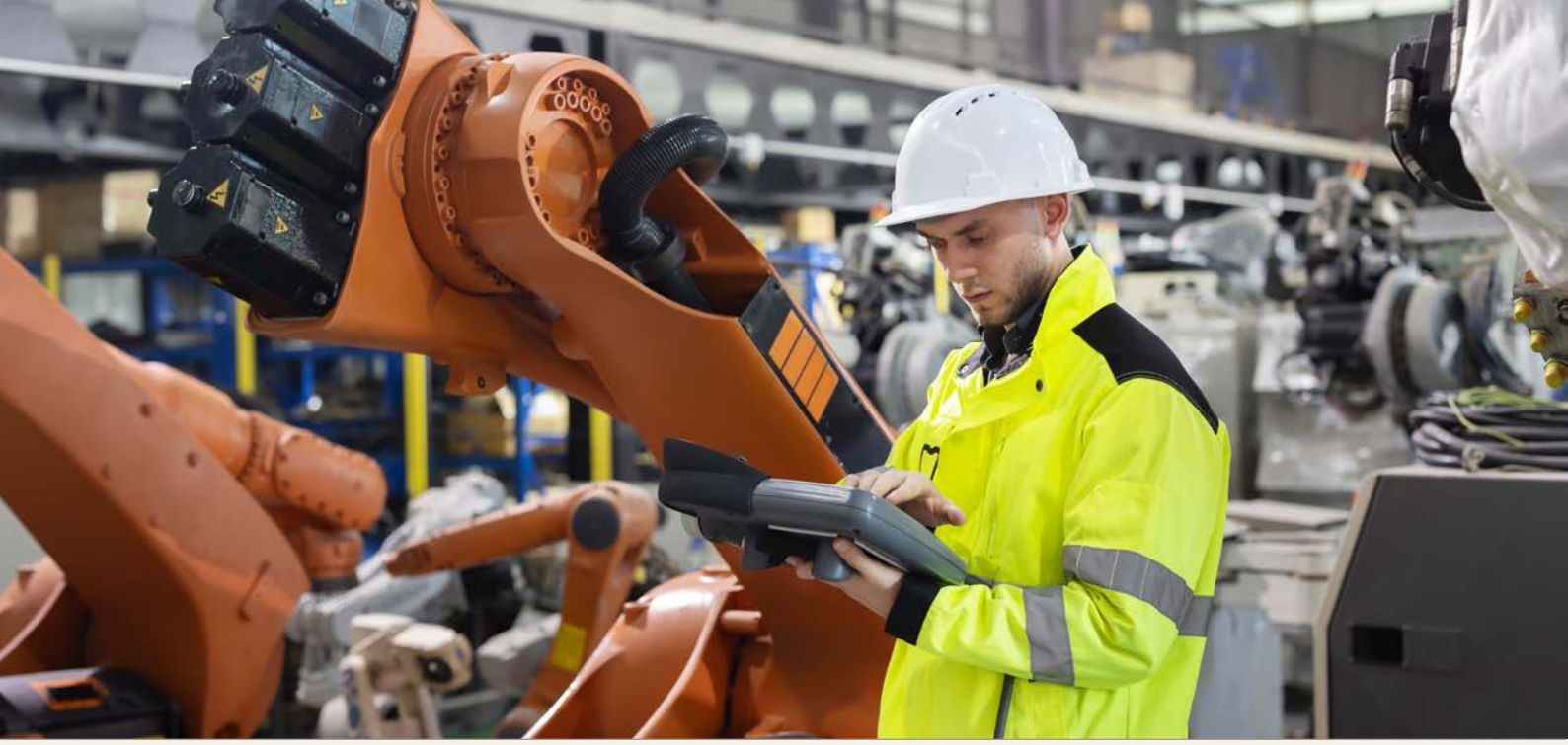
Policy transparency is essential

To meet client needs effectively, brokers are calling for a mandate of policy transparency. Currently, key cover elements such as PCI fines, invoice fraud, and data restoration costs are not always clearly labelled. Furthermore, valuable differentiators like 72-hour Service Level Agreements (SLAs) or the waiving of excesses for using approved vendors might be “hidden in the wording” or grouped under vague headers like “cyber event”. When these features are buried, they are less understood by brokers and go unrecognised by the client, reducing the perceived competitiveness and value of the policy.

A major technical differentiator that has emerged in this research is the split between “Any One Claim” (AOC) and “Aggregate” limit structures. Brokers are increasingly asking for AOC policies, which provide a full reinstatement of the limit for every incident. Because cyberattacks are rarely isolated events, aggregate limits (which are still common among major composite insurers) can leave a business dangerously underinsured if they suffer multiple incidents, such as a ransomware attack followed by an invoice fraud event in a single year.

Meeting client needs requires a greater shift toward plain English wordings and clearly defined limit structures. Brokers want to confidently explain to a client exactly how the policy will respond in a crisis. Providing this level of clarity allows the broker to defend the value of the product and move the conversation away from the “lowest price” mindset.





Value-adds

Brokers told us that value-adds are crucial for advocacy and post-sale satisfaction. While they may not win the deal alone, tools like training, live threat monitoring and funded PR services offer support outside of the main cover elements.

That's why our proposition includes a comprehensive suite of value-added services to support businesses when they need it most – before, during, and after a cyberattack occurs.

Pre-breach, Markel provides access to cyber scanning technology, offering a continuously updated view of the policyholder's cyber risk, along with the cyber risk management toolkit, helping businesses prepare for, respond to, and recover from cyber incidents.

Additional support includes access to cyber and claims webinars, delivered by Markel experts, in addition to a contract review service from Markel Law, allowing businesses to identify potential cyber exposures within IT supplier contracts, as well as a regulatory compliance webinar, designed to help businesses understand evolving legal and regulatory requirements.

Post-breach, policyholders have access to a range of specialist support services to minimise disruption, aid recovery, and help businesses return to normal operations as soon as possible. This includes 24/7 access to Incident and breach response services, emergency cyber specialists who can support within minutes of an incident being reported.

Support continues beyond the immediate incident, with claims handled by our award-winning claims team, and post-breach remediation services to help businesses understand the cause of an attack, identify vulnerabilities, and reduce the likelihood of a similar incident occurring in the future. Together, these services not only help businesses recover from cyber events but build resilience and emerge stronger.

Understanding broker pain points in the cyber sales journey

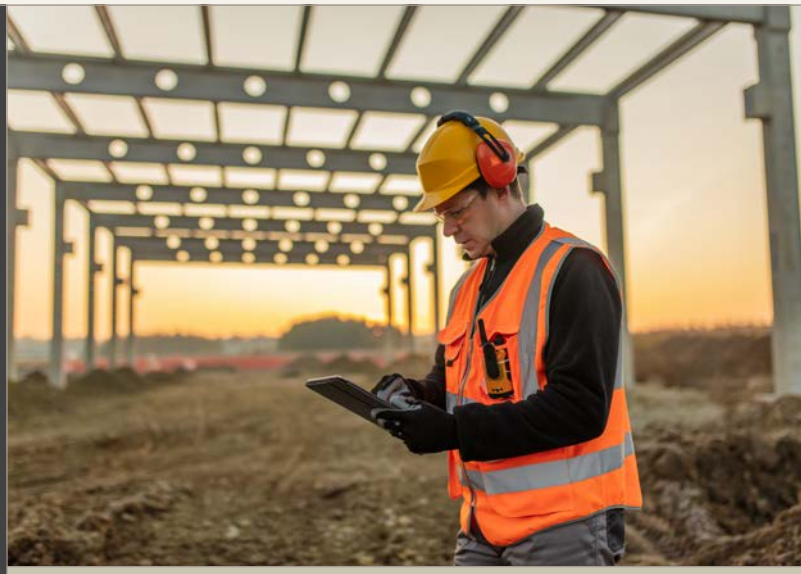
Understanding broker pain points was a key element of the research and we aimed to evaluate this in two distinct ways: pain points when talking to customers and friction within the customer sales journey.

Pain points when talking to customers

Triggered interest via contracts or incidents

Many SMEs only consider cyber cover after a contract demands it or following a scare. It's reactive rather than strategic.

"We're seeing more and more that contracts, particularly where **clients need to sign third party contracts**, are asking for **cyber-specific terms** or they've had a skirmish with a cyber incident and they're now thinking, what can I get to protect myself against this?"





General low awareness and market penetration

Even with growing awareness, actual take-up remains low. Brokers highlight that many SMEs still don't see cyber as a priority.

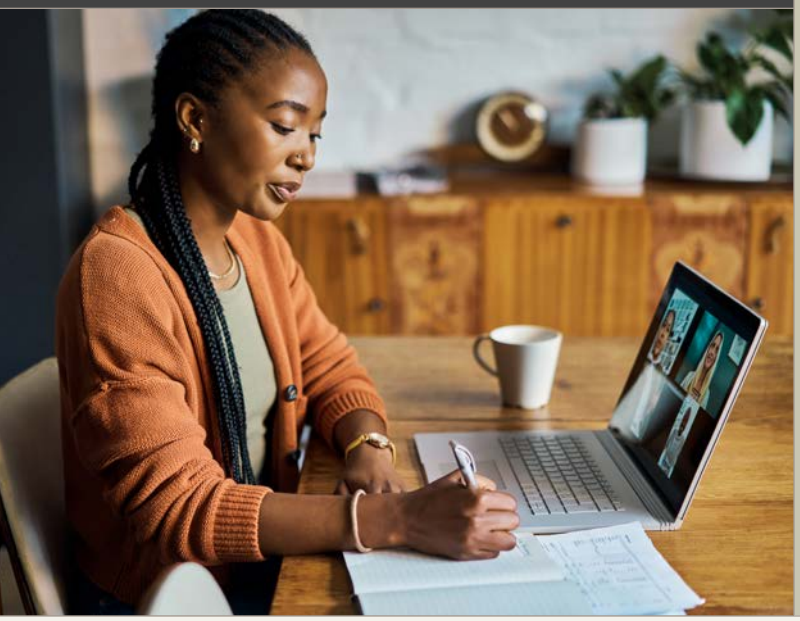
"I think awareness has gone up over the last few years, but **the penetration rate for cyber insurance is still pretty low. It's probably about 15% overall.**"



Sector-specific awareness

Certain industries (e.g. financial, tech, healthcare) are more clued up about cyber threats and risks.

"So, some sectors, things like financial, tech, healthcare, education, those kind of risks that are really heavily targeted quite often are perhaps a bit more aware than others."



Risk vs premium trade-off based on business maturity

Cyber cover is often evaluated by clients in terms of ROI, especially in early stages of their business lifecycle.

"I think people in our sector are very aware it's a big risk to businesses in terms of how things can go wrong. It's always a case of weighing up risk versus premium and it depends on where they are in their business journey."

Confusion about cover and limitations

Clients mistakenly believe they're already covered, or don't understand the limits of bundled or vague policies.

"I think a lot of people think they have cover and packages. But really, it's either very low limits and not covering very much, or they actually don't have it at all... they think, oh, our public liability covers a bit of data breach stuff. So therefore, that's cyber, but it's not really."



Broker confidence with technical questions

Some brokers feel under-equipped to explain the more technical aspects of cyber insurance to their clients.

"I'm advising my clients why they need something, but I'm not technical enough to know what all the answers are."

The insurance sector's efforts to protect a greater number of businesses against the threat of cyber risk are hindered by several ingrained pain points.

The market remains largely reactive, with many businesses only considering cover when contractually mandated or following a direct "skirmish" with a digital incident. This, coupled with a perceived market penetration rate of just 15% by some, highlights a significant gap between general awareness and the purchasing decision.

For many firms, that decision remains a transactional trade-off between risk and premium, heavily influenced by the business's current maturity and stage of growth.

A major barrier to conversion is the misconception of existing cover, where many SMEs mistakenly believe they are protected through other insurances. This confusion is exacerbated by the confidence gap, with every broker interviewed noting that they sometimes feel they are "not tech enough" to handle the technical questions posed by savvy clients.

Bridging these gaps requires a greater degree of technical education that allows brokers to confidently communicate the threat of cyber risk and how insurance offers wide-ranging protection.

Friction within the customer journey

STAGE	WHAT HAPPENS	COMMON BROKER FRICTION
Awareness	Broker introduces cyber insurance or SME client hears about it elsewhere	Client believes cover is only for big firms or tech companies
Interest	Client shows curiosity, asks for more information	Limited understanding of what's covered; assumed it's expensive or complicated
Consideration	Client begins weighing options, looking at cover levels, value and risk	Hard-to-compare wordings; lack of standardisation across insurers
Intent	Client is keen, asks for a quote or specific product details	Proposal forms seen as off-putting or excessive; client delays or drops off
Evaluation	Final review of insurer choice, cover and service	Broker struggles to differentiate between providers; client need simplicity or reassurance
Purchase	Policy bound; documentation issued	Lack of clarity in how to activate support services; broker left to interpret wordings
Post-sale	Claims handling, service usage, renewal	Client doesn't use value-add tools; renewal seen as a grudge purchase unless there's a claim

From a broker's perspective, the cyber sales journey is rarely a simple transition from lead to onboarded policyholder. In reality, it is a consultative process with the potential for friction points at every stage.

In the initial Awareness and Interest phases, the "not me" belief is commonplace, where SMEs view cyber protection as mainly for larger organisations.

As the sales journey moves toward Intent and Evaluation, operational friction can arise, with overly complex proposal forms often off putting and a lack of standardisation in wordings making it difficult for brokers to provide the clear, comparative advice clients need.

Our research further identified post-sale disconnect where clients often feel they lack the information on how to activate the purchased support or value-add services. When these go unused, the renewal is ultimately reduced to a "grudge purchase".

Conclusion

The findings within our Cracking the Cyber-Market Code research report highlight the "value gap" in the UK cyber insurance market. While SMEs are aware of digital threats, their desire to purchase protection against this is often affected by overly technical jargon and a misunderstanding of their firm's own digital vulnerability.

Unlocking the estimated untapped 85% of the market will depend on transparency for customers and proactive support offered by insurers. By removing the operational friction points identified in this report and providing a clear service and claims promise, the insurance sector can create the environment where SMEs are more likely to purchase cyber cover, protecting themselves and the wider business community in the process.

Why choose Markel as your Cyber insurer?

Market-leading features and cover that goes beyond the policy wording.

Built to address the realities of modern cyber risk, our Cyber Insurance solution combines specialist cover with broader business interruption services and practical support services.

The highlights below showcase some of the market-leading features and key cover enhancements that policyholders can benefit from if you choose to place your cyber business with Markel.

These features are designed directly from feedback from brokers like you, to help you sell Cyber with confidence to UK SMEs, and ultimately to help businesses build resilience and recover more effectively from cyberattacks.



General cover and claims approach

Any one claim
Our Cyber policy operates on an any one claim basis, meaning the policy limit applies separately to each covered claim, rather than being shared across multiple claims. As cyber incidents become increasingly more costly and complex, this provides clients with greater certainty and peace of mind that meaningful protection is available when it matters most.

Nil deductible available
We also offer a nil deductible option, helping businesses access support quickly without the barrier of an excess.



Business interruption covers

Non-IT critical service provider business interruption
Our cyber insurance policy helps protect against disruption extending beyond a client's own systems, including cyber incidents affecting critical non-IT service providers such as payroll, hr, logistics and outsourced administration partners.

Dependent customer business interruption
The policy also includes dependent customer business interruption cover, protecting against loss of income when a key customer suffers a cyber incident. Cover is automatically included with a £25,000 blanket limit and can be increased for named customers where required.

Loss of stock
Loss of stock cover helps protect businesses if a cyber incident results in damaged, spoiled or unusable stock.



Legal and liability covers

Technology services liability
Cover that protects businesses providing technology products, services or advice against claims arising from alleged errors or failures.

Contingent bodily injury
Our cyber insurance policy recognises that cyber incidents can have physical consequences, providing protection where bodily injury results from a cyber-related security failure.

Management liability
Protects directors and senior leaders against claims arising from decisions made while running the business, helping cover legal costs, settlements and awards resulting from alleged wrongful acts.

Media liability
Provides protection against claims arising from digital content, marketing activities and media publications, including allegations such as defamation, infringement of intellectual property rights and other media-related liabilities.

Regulatory investigations and fines
Helps businesses manage the financial impact of regulatory investigations following a cyber incident, covering defence costs and insurable fines and penalties where legally permissible.

PCI DSS investigations and fines
Supports businesses that handle payment card data by covering the costs associated with PCI DSS investigations, assessments, fines and penalties arising from a security breach or cyber incident.

Value-added services

Incident and breach response
Rapid remediation of cyberattacks, get advice on how to avoid further damage within 15 minutes from the emergency response team 24/7.

Contract review service
Our Markel Law specialists assess customer and third-party contracts against a number of cyber-focused obligations, providing practical recommendations to address weaknesses that could otherwise increase liability, and which will help clients build resilience against cyber incidents.

Cyber risk management toolkit
Helps your business prepare for, respond to and recover from cyber incidents with breach support, threat intelligence, cyber risk tools and employee training

Business Hub
Policyholders also benefit from business hub, a one-stop shop for practical guidance, templates, training materials and business support tools, alongside 24/7 expert support through the business and legal helpline.

Post-breach remediation costs
We cover the cost of expert post-breach assessments and training to help you understand what happened, identify areas for improvement, strengthen your cyber defences, and reduce the risk of future incidents.

Privacy policy review
Annual complimentary review of your privacy policy by a specialist lawyer at Markel Law, ensuring it meets your current data processing activities and complies with good industry practice and any recent legislative or regulatory reforms in the law of England and Wales. The review includes feedback and recommendations on any areas where revisions should be considered.

Regulatory compliance webinar
In addition, clients have access to a regulatory compliance webinar delivered by markel law. Backed by close collaboration between markel law and our specialist claims teams, clients benefit from joined-up support at every stage, from risk mitigation and compliance guidance, through to claims handling and recovery.

Additional covers

Betterment
Our cyber insurance policy includes extensions designed to support businesses before, during and after a cyber incident. Betterment cover provides certainty when replacing damaged systems with upgraded technology, without percentage restrictions commonly applied elsewhere.

Crisis response costs
We will extend cover for any crisis response costs as a result of any security or system failure. No retention shall be applicable and costs will be provided for 48 consecutive hours after notification to the cyber response party and do not require our prior consent.

Tender disruption
The policy also includes tender disruption cover, helping protect businesses from the financial impact of missed tender opportunities caused by a cyber incident.

Award-winning claims service

Consistently rated 5-star service
With recognition for achieving a 5-star service ranking for seven consecutive years and a market-leading net promoter score (NPS) that reflects broker trust, we consistently deliver exceptional outcomes through reliable support, specialist expertise and strong partnerships.

Claims resolved in a single interaction
Wherever possible, our empowered claims handlers aim to resolve straightforward claims in a single interaction, thanks to elevated settlement authorities across our team, helping protect your clients' businesses with minimal delays.

MARKEL

All information accurate at the time of production August 2026.

For broker/intermediary use only. Not for distribution to customers or the public, and not to be relied upon by customers. This document is provided for general information to support intermediary understanding of Markel's Cyber proposition and does not constitute advice, a personal recommendation, a policy document, or customer-facing financial promotion. Intermediaries are responsible for ensuring any customer communications are fair, clear, and not misleading and comply with applicable FCA requirements. Cover is subject to underwriting, policy terms, conditions, limits, and exclusions. In the event of inconsistency, the policy wording prevails.

Markel (UK) Limited is an appointed representative of Markel International Insurance Company Limited (Reference number: 202570), which is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority.

Registered Office: 20 Fenchurch Street, London, EC3M 3AZ. Registered in England No. 2430992.

Calls from a landline will be charged at your local rate. Calls from mobile phones are charged at your local rates in accordance with your tariff.