

BRIT

# A Turning Tide:

## How growth and AI are driving SME action on cyber

As SMEs grow, cyber resilience is becoming increasingly important to protecting operations, meeting client expectations and securing future opportunities.

**64%**

now describe cyber security as a top or high priority

**51%**

say recent high-profile attacks have changed how they think about cyber risk

**79%**

believe AI is making attacks more sophisticated and harder to prevent

**68%**

say AI makes them more likely to purchase cyber cover

**45%**

plan to increase cyber-security spending



**A THIRD**

believe their business might not survive a cyberattack

**A THIRD**

still provide no cyber-security training to employees

## EXECUTIVE SUMMARY

The cyber protection gap for SMEs has been well documented, and the industry has been taking meaningful steps to increase awareness of the risk landscape and the protection that is available.

What we're seeing now is that the tide is starting to turn. As SMEs set their sights on growth, cyber resilience is fast becoming essential not only to managing risk but to protecting their ambitions to scale. That shift is being accelerated by a recent string of high-profile cyberattacks, and rapid advancements in AI technology, which together are driving a fundamental shift in how businesses think.

Our survey of 500 UK SME leaders explores how these core drivers are reshaping SME appetite and awareness, finding that 64% of SMEs now describe cyber security as a top or high priority. Half of businesses (51%) say recent high-profile attacks have changed how they think about cyber risk.

In the age of Artificial Intelligence, 79% also say that AI is making cyberattacks more sophisticated and harder to prevent, and 68% say it is making them more likely to purchase cyber cover.

There are encouraging signs that this awareness is also beginning to influence business decisions, with growth proving a powerful catalyst for action. Over a third of SMEs who do not currently hold cyber cover say they are very likely to take out a policy in the next year, and 45% are planning to increase their spending on cyber security. As businesses grow, they have more to protect, and cyber resilience is increasingly seen as the foundation that allows them to scale with confidence rather than expose themselves to setbacks.

That said, while SMEs are becoming more alert to cyber risks and intention for action is there, this alone does not create resilience. While 42% of SMEs believe their cyber risk has increased over the past 12 months and 74% plan to respond in some way in the next year, barriers still exist between intention and meaningful implementation. With awareness building, now is the time to ensure SMEs are making informed choices around cyber insurance that support their resilience and their growth in the face of an ever-evolving risk landscape.

**ADELLE GRUBER CLASS UNDERWRITER, CYBER & TECHNOLOGY**



## GROWTH AS A CATALYST FOR ACTION

For UK SMEs, business growth and cyber security are increasingly inseparable. Yet as companies look to scale and capture new opportunities, investment in the right systems and security often doesn't keep pace.

### SMEs say




Nearly two fifths of SMEs admit that their cyber security is unprepared to keep up with growth. A figure that climbs to over half (58%) among the smallest SMEs[1].

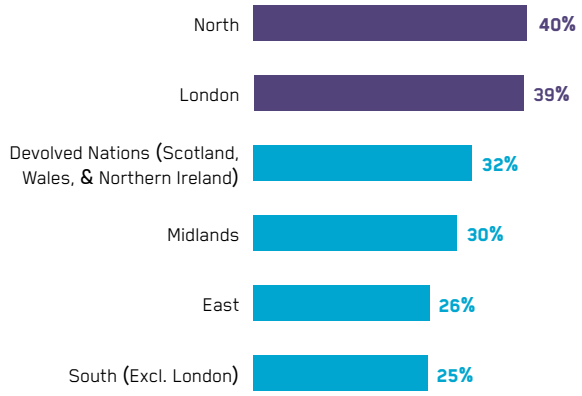
Businesses are also **feeling nervous about the impact a cyberattack could have on their long-term viability.**

# A THIRD

of SME decision makers fear their business would not survive if faced with a cyberattack.

### % per region believing their business might not survive a cyber attack

This is particularly acute for businesses based in the North of England (40%) and London (39%).




# 43%

It is perhaps no surprise then, that among SMEs planning to increase their cyber security spending, 43% cite business growth itself as the primary driver.

# 55%

This is further reinforced by the fact that 55% of SMEs say that their larger clients now expect them to meet their cyber security standards.

### KEY TAKEAWAY

**Research finding:**
Reliance on secure systems increases with business growth.

**Why it matters:**
Cyber resilience is becoming essential to winning and retaining business.

**The resilience gap:**
Security investment is not always keeping pace with growth.

**Broker implication:**
Make cyber part of every client growth conversation.

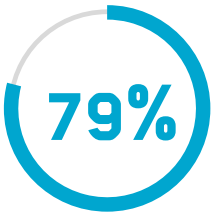
**The Broker Conversation** As your client grows, which systems, suppliers or digital processes are becoming more critical to its ability to trade?

[1] SMEs with less than £500k in annual turnover

## The AI effect

It is hard to avoid the ongoing newsflow around advances in AI and how this is changing both the risk environment and how businesses and consumers operate.

### SMEs say

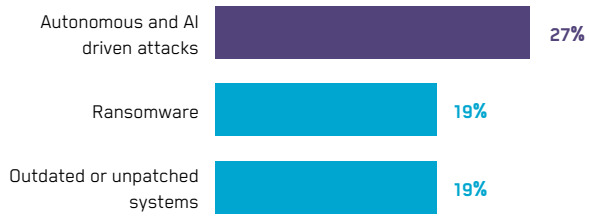



When asked, 79% of SMEs agreed that AI is making cyberattacks more sophisticated and harder to prevent.




68% also say that as a result, AI has made them more likely to purchase cyber insurance.

While we have become familiar with terms like phishing and malware, **27%** now see **autonomous and AI driven attacks** as presenting the greatest risk to their business' cyber security, coming in above **ransomware (19%)** and **outdated or unpatched systems (19%).**




We have seen AI dramatically reduce the barrier to entry for threat actors, and given its increasing presence in daily life, it is little wonder that it is so front of mind. Yet while the threat landscape evolves, strong fundamentals and robust controls are still among the most effective tools for reducing risk in the age of AI. Cyber insurance plays an important role here, extending well beyond financial cover into proactive risk management. The right policy is not simply a safety net for when things go wrong. They're about preparing and protecting, and helping businesses access tools and services that make an attack less likely in the first place.

But it's not all about AI and autonomous technology. SMEs also rank **employee human error**, such as clicking phishing links or weak passwords, in the top three greatest risks to their business' cybersecurity (30%). Yet a third still do not train their employees on recognising and responding to these threats.

This is again where cyber insurance can help. Brit's cyber risk management services include employee and phishing training, as well as incident response planning and cyber fitness checks as part of policies.

More often than not, employees can be your first line of defence in protecting against cyber threats.

### KEY TAKEAWAY

**Research finding:**
AI is increasing concern and appetite for cyber cover.

**Why it matters:**
Attacks are becoming faster, more convincing and easier to scale.

**The resilience gap:**
A third of SMEs still provide no cyber-security training.

**Broker implication:**
Focus conversations on people, controls and verification.

**The Broker Conversation**

How would your client verify an urgent payment request if the email, voice message or video appeared genuine?

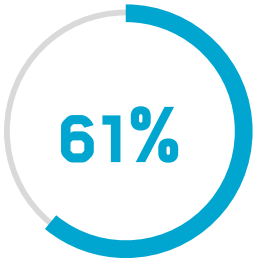
This helps your client consider the level of awareness their staff has, what training they need and what processes should be in place to mitigate the risk.

## SME's role in the supply chain

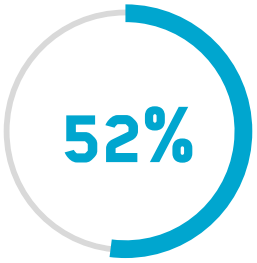
SMEs are increasingly recognising their role in broader cyber ecosystems. As we've seen from high profile incidents, in manufacturing and retail, cyberattacks can stretch much further than just the organisation that has been attacked.

This is something SMEs are increasingly aware of.

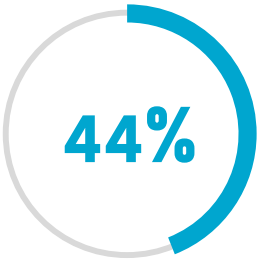
### SMEs say




When polled, **61% said they could be held responsible** if a cyberattack on them disrupted a customer's business.




**Over half (52%) acknowledge attackers could target them** to reach larger clients.




**44% also fear a supplier attack** could stop them from trading.

Supply chain risk can be unavoidable. Even if the breach begins elsewhere, the disruption can quickly become the SMEs responsibility to manage.

Yet despite awareness, the lack of investment in cyber security and training means SMEs can often remain a weak link in the supply chain.

### KEY TAKEAWAY

**Research finding:**
SMEs recognise that cyber risk extends across customers and suppliers.

**Why it matters:**
One incident can disrupt organisations throughout the supply chain.

**The resilience gap:**
The disruption can become the SMEs responsibility.

**Broker implication:**
Explore the client's most critical customer and supplier dependencies.

**The Broker Conversation**

How would your customers be affected if access to your systems disappeared for a week?

This helps the client think about their role in the supply chain and their ability to serve their customers

## Barriers to purchasing cover differ by SME size

### SMEs say




Cost remains one of the most frequently cited barriers to SMEs purchasing cyber cover, **with price ranking as the single most influential factor (55%) when selecting a provider.**

This focus on cost is reflected in how businesses resource their security more broadly, as **more than a third of SMEs** have no dedicated budget or team for cyber.

In reality, the financial impact of a breach almost always exceeds the cost of a cyber insurance policy. Government research indicates that the average recovery cost for a small business following a serious breach is close to £8,000, though the real figure can exceed £50,000 once downtime, reputational damage, and lost income are accounted for.

**Real claims do not follow neat averages**

In 2026, we reserved

**£350,000** on a cyber claim where the annual premium was less than £3,500. A reminder that significant cyber losses are not limited to large organisations or high premium policies.



## Rising awareness is influencing business decisions

### SMEs say




Larger SMEs[2] are concerned that claims will not be paid or believe that they're already protected elsewhere.

**In fact, 26% of all businesses believe cyber may already be covered by another insurance policy, or that they are protected by their IT provider.**

However, many traditional small business insurance policies don't offer coverage for cyber incidents such as breaches or attacks. Firms may also fall victim to 'silent cyber', where coverage may not be clear, leaving gaps in protection. This can lead to ambiguity and uncertainty about whether insurance products provide coverage for cyber perils. Having a cyber insurance policy means you can ensure affirmative cover is provided.

Importantly, a specific cyber policy includes access to training and support services essential to reducing cyber risk before a breach, and legal, digital and negotiation expertise during and after a breach.

Businesses must also avoid falling into the assumption that outsourcing IT requirements removes the direct risk. In reality, business are still responsible for their customer data, contractual obligations, and day-to-day operations, irrespective of outsourcing arrangements.

### SMEs say




Holding little sensitive data is a core reason for not purchasing cyber cover (26%)

**36%**
This is particularly the case for smaller SMEs.

Yet, cyberattacks don't just stop at data loss. Core systems and processes can be compromised during an attack, impacting stock, order fulfilment and the ability to make and receive payments among other things.

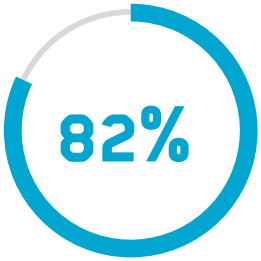
Employee data and supplier details are also attractive to attackers, who can profit from even small-scale breaches.



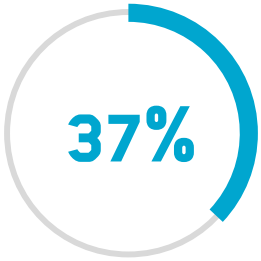
[2] SMEs with over £50m in annual turnover

## Rising awareness is influencing business decisions

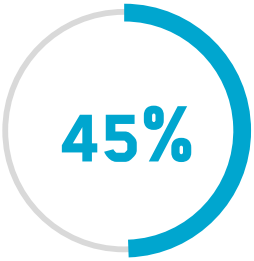
### SMEs say




In the current risk environment, **82%** of SMEs who hold cyber insurance are likely to increase their cover over the next year



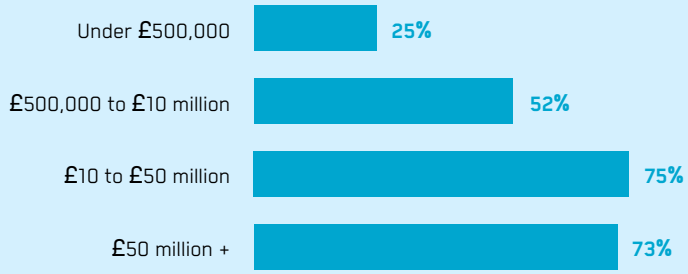

**37%** of SMEs who don't hold cyber insurance are very likely to take our a policy in the next year




**45%** plan to increase their spending on cyber security, predominantly driven by the growing threat of cyberattacks. This is particularly the case for SMEs with revenues over £500,000.

The appetite to invest in the UK varies notably by region. London leads the way, with 56% of SMEs planning to increase their cyber security spend, closely followed by the North at 50%. These two regions stand out as the clear front-runners nationally. Followed by the Midlands (42%), the South (40%), and the Devolved Nations (33%).

**Plans to increase spending on cyber security by company revenue**




### KEY TAKEAWAY

**Research finding:**
Cost, limited data and outsourced IT remain significant barriers.

**Why it matters:**
Cyber incidents can affect operations, income and customers, not just data.

**The resilience gap:**
SMEs may recognise the risk without understanding their full exposure.

**Broker implication:**
Identify the barrier, then connect it to the client's business dependency.

**The Broker Conversation**

Is your client's main barrier price, perceived lack of exposure, confidence in its IT provider, or uncertainty about what cyber insurance actually provides?

- If it's price, talk about the cost of a breach or attack
- If it's lack of exposure, talk about the impact of system downtime
- If it's outsourced IT, talk about the responsibility remaining with the client
- If it's uncertainty about cyber insurance, talk support before, during and after and incident.

## Starting the cyber conversation and turning awareness into action

**01**

### Start with business continuity, not cyber terminology

Ask what the business relies on to trade, pay, communicate and serve customers.

**02**

### Treat growth as a risk conversation

Growing SMEs are adding technology, customers, suppliers and contractual expectations, sometimes faster than their controls develop.

**03**

### Turn AI attack anxiety into practical questions

Focus on payment verification, account access, employee awareness and decision-making.

**04**

### Explore the whole supply chain

Discuss both the SME's responsibility to customers and its dependence on critical suppliers.

**05**

### Identify the real buying barrier

Price, outsourced IT, limited data and misguided confidence in other insurance are valid concerns that can be easily addressed.

## Methodology

Brit Insurance commissioned an online survey of 500 UK-based small and medium-sized enterprises (SMEs), conducted between 19 and 27 August 2026. Respondents spanned the full SME spectrum, from micro-enterprises (1–9 employees) to larger SMEs at the upper end of the bracket (100–249 employees).

Respondents were drawn from across the UK and covered a broad range of sectors, including Construction, Retail and Hospitality and Professional Services, alongside Healthcare, Education, Manufacturing, Financial Services and others. To ensure the findings reflect informed, business-level views, the survey targeted senior decision-makers including business owners or founders, senior managers and heads of function, C-suite executives, and board members, directors or partners.



## DISCLAIMER

This document provides examples of incidents and does not constitute an expression of coverage under any insurance product. This is not a solicitation or offer for insurance. Coverage is only available from licensed brokers. Coverage is subject to the full terms and conditions of the policy



**GET IN TOUCH:**

britinsurance.com/cyber

BRIT