CyberSmart

The CyberSmart MSP Survey 2026

Introduction

Managed service providers (MSPs) and managed security service providers (MSSPs) play an important role in the global economy. For simplicity, we'll refer to both collectively as MSPs from here onwards.

Research from the UK government's Department for Science, Innovation and Technology (DSIT) revealed that, as of 2025, there are 12,867 active MSPs in the UK (up from 11,492 in 2024). Collectively, these MSPs are estimated to generate around £51 billion in annual revenue and employ over 343,762 individuals.

However, MSPs represent more than just a lucrative part of the UK economy. For many small businesses, MSPs are seen as a critical first line of defence against cyber threats. They offer time, knowledge and resource-strapped SMEs a one-stop shop for many of their IT needs, providing and administering everything from network security and cybersecurity awareness training to office software packages. This also makes them a critical part of the supply chain.

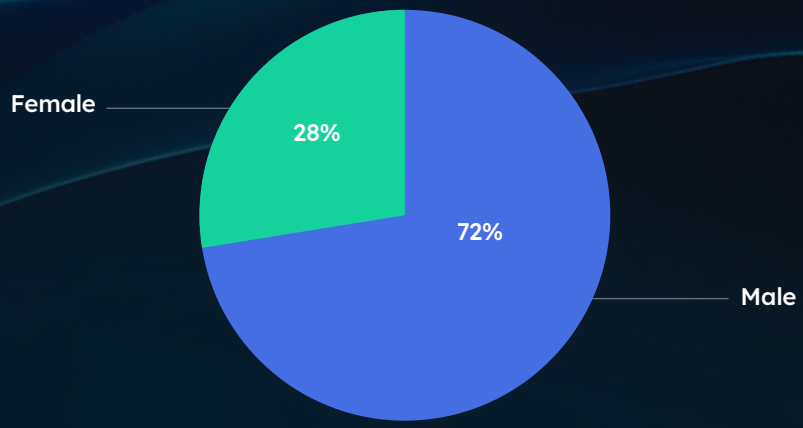
However, the same things that make MSPs a cornerstone of our economy also make them a valuable target for cybercriminals. As trusted partners to hundreds of thousands of UK businesses, MSPs typically have access privileges to clients' infrastructure and inner workings. By gaining access to an MSP, a malicious actor potentially has access to a wealth of sensitive knowledge on both the MSP itself and its customers. What's concerning is that, of all the MSPs we surveyed, 75% had suffered at least one breach in the past 12 months.

For the first time, UK regulation has recognised the importance of MSPs within the supply chain. The Cyber Security and Resilience Bill, anticipated in 2026, brings medium and large MSPs under direct regulation. It targets entities with roughly 50+ employees and £10m+ turnover, mandating strict 24-hour incident reporting, security audits and potential £17m+ fines for non-compliance. This step marks a notable shift in how historically overlooked MSPs are viewed, but does it go far enough?

That's one of the questions we set out to explore with the third annual CyberSmart MSP Survey. For 2026, we've teamed up again with OnePoll to ask MSPs key questions about their cybersecurity, as well as pressing topics such as regulation and the supply chain. How well defended are these organisations? What do they feel are the biggest threats facing them and their customers? And, with cybersecurity legislation finally recognising the importance of these entities, how are they preparing?

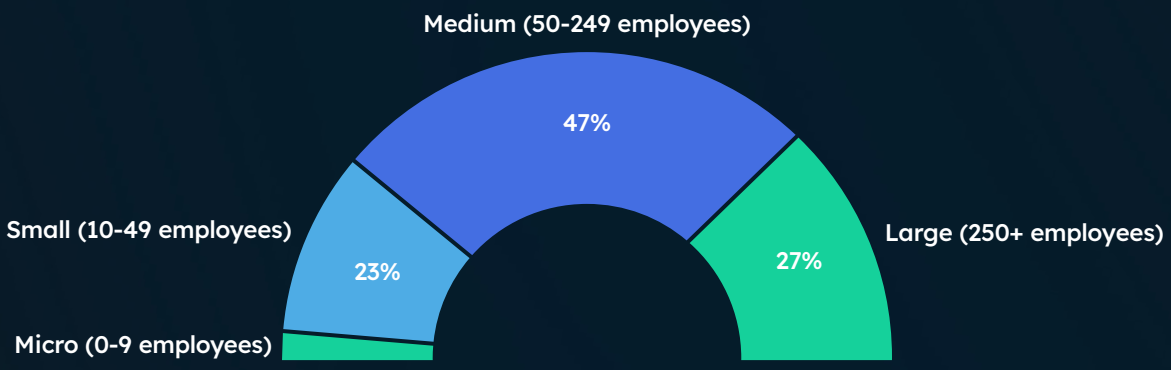
The 2026 edition features insights from 350 MSP leaders across the UK and Ireland, spanning a selection of industries and serving customers ranging from 1 to 250+ employees.

Are you...?



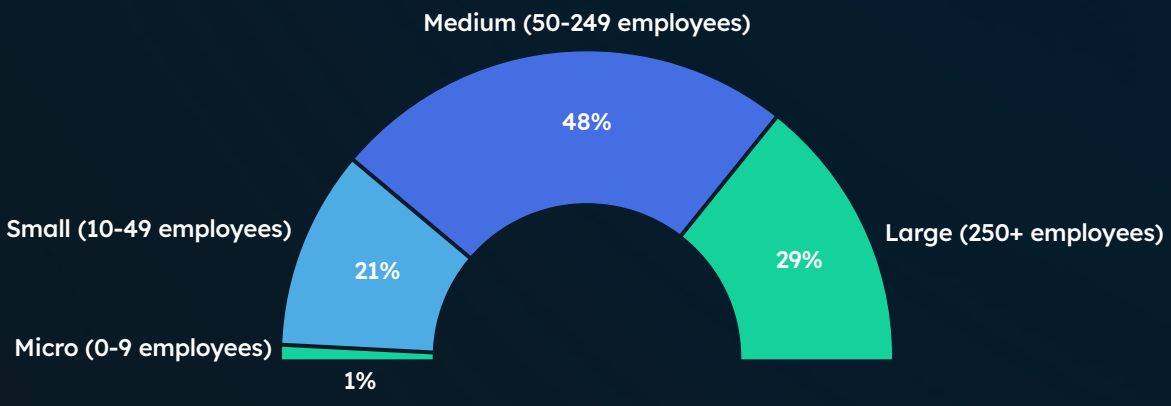
Response count 350

What most accurately describes the size of the organisation you currently work for? [Select best match]



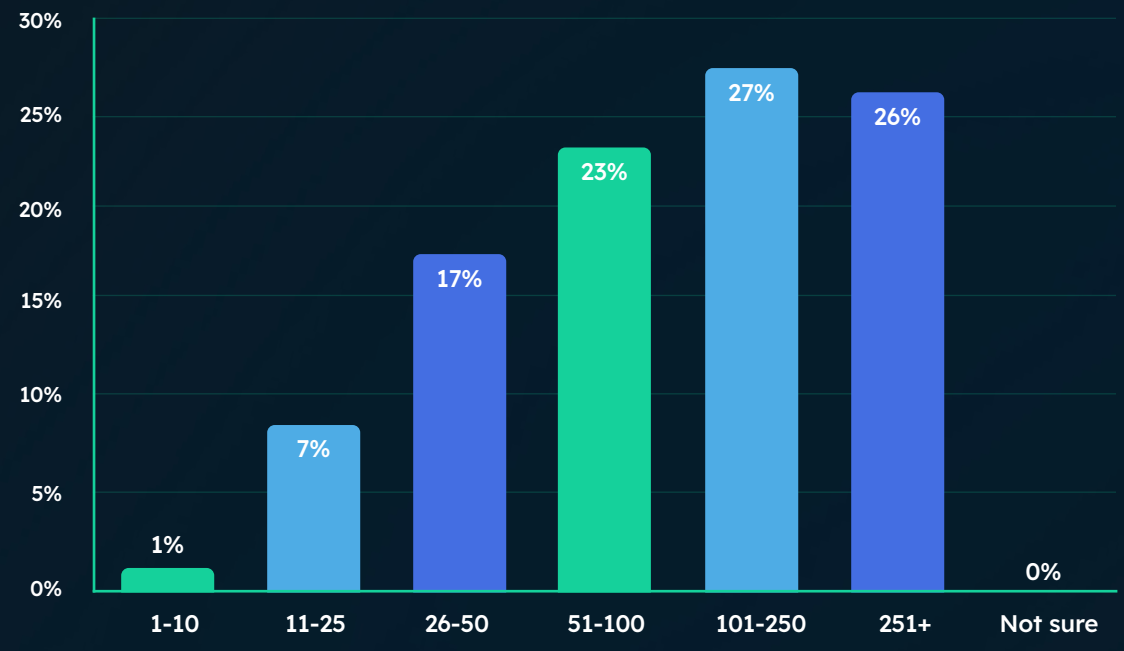
Response count 350

What most accurately describes the average company size of your customers? [Select best match]



Response count 350

How many customers do you currently have in total? [Select best match]



Response count 350

What follows are the results of this study, providing an accurate picture of the cybersecurity landscape for MSPs and their customers in 2026.

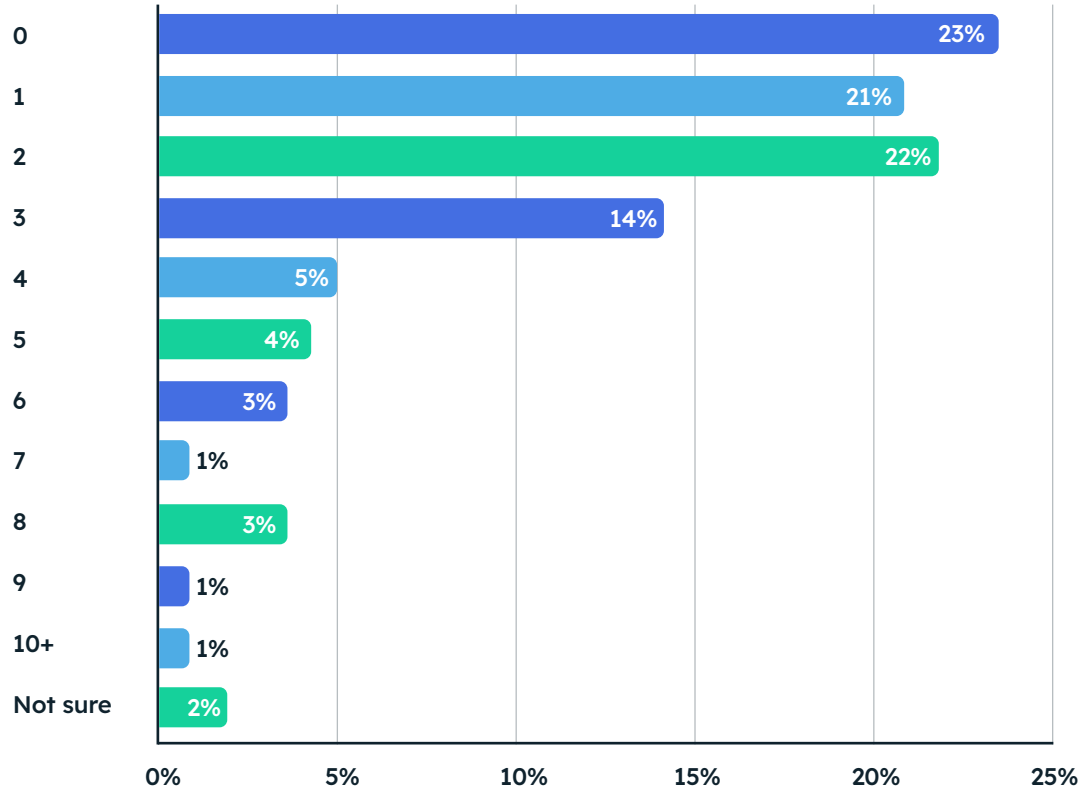
Repeat Breaches on MSPs are Now Commonplace

Over the past year, we've continued to see high-profile breaches affecting MSPs, as well as the wider ecosystems they operate in. In early 2026, a global cloud marketplace and distribution platform for MSPs **disclosed a data exposure incident** impacting around 1,800 MSP customers, emphasising the downstream supply chain risk.

Additionally, one large provider faced ongoing regulatory fallout in 2025-2026 following a major breach. This resulted in a £14m fine from the **Information Commissioner's Office**. Meanwhile, ransomware groups continue to target MSP tools, particularly RMM platforms, to scale their attacks.

Beyond these headline incidents, our survey uncovered evidence that breaches of MSPs are widespread, with the majority (75%) of MSPs having been breached at least once in the past year.

How many cybersecurity breaches, if any, has the business you work for suffered in the last 12 months?



Response count 350

Worryingly, of the 350 MSP leaders we surveyed, 54% reported being breached two or more times in the past 12 months. Additionally, nearly a third (32%) of respondents admitted to experiencing three or more breaches. This shows that repeat breaches are still concerningly commonplace.

In 2026, breach frequency eased slightly versus previous years, but not enough to change the picture much. In 2025, 69% of MSPs reported being breached two or more times (67% in 2024) and 47% reported being breached three or more times.

The downward trend demonstrates that MSPs are taking their own security seriously and becoming more effective at blocking attacks.

Of course, it's worth noting that "a breach" can mean anything from a minor incursion to business-critical data or systems being compromised. Many of the incidents reported are likely to be the former. However, these figures still remain uncomfortably high.

Is Customer Risk Stabilising?

From “the costliest cyberattack in UK history” on a **major manufacturer** to one **158-year-old logistics firm being forced to shut down** after a cyberattack, the past year has highlighted the far-reaching impact a single breach can have on an entire organisation, or, in some cases, an entire economy.

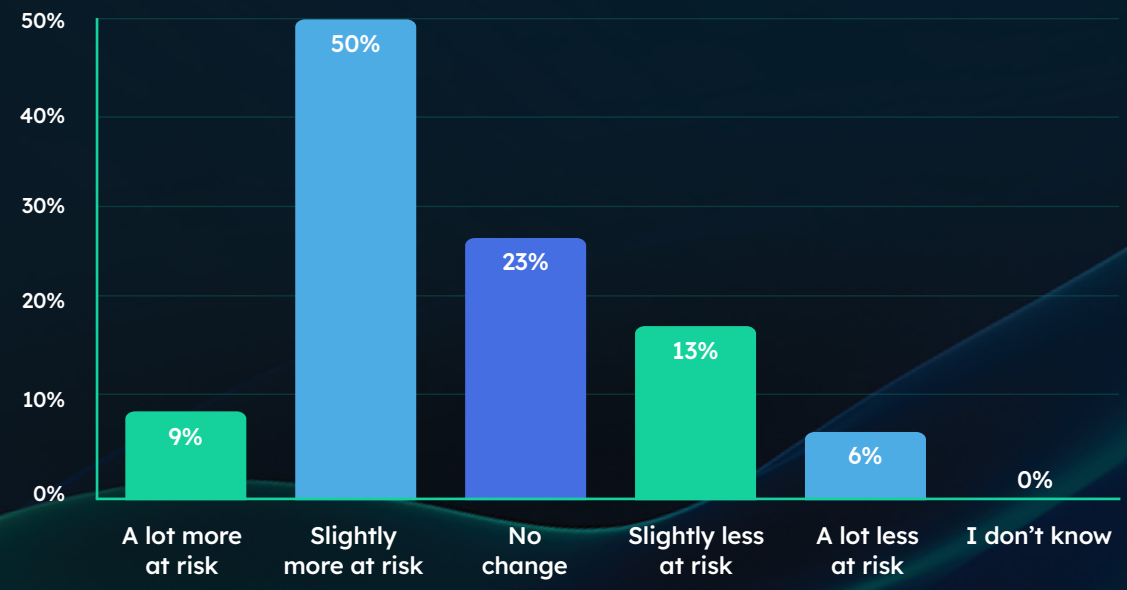
So it’s no surprise to see that MSP leaders are about as concerned for their customers’ cyber safety as they have been over the past two years. 59% of MSPs feel that their customers are more at risk in the last 12 months than they previously were; this was 58% in 2025 and 61% in 2024.

However, what is interesting is that the percentage of MSPs who sense no change in risk level over the last 12 months has almost doubled (from 12% to 23%).

This points to a growing divide in how MSPs perceive risk. While a consistent majority continue to feel their customers are at greater risk, a notable and rising proportion now see no real change in the threat landscape.

In other words, MSPs are increasingly split between those who believe risks are still escalating and those who feel the situation has stabilised. We’ll explore the drivers behind this sense of stability later in the report, but first, let’s turn to the emerging threats shaping the more cautious outlook.

Do you feel your customers are more or less at risk from cyber threats in the past 12 months than they were previously?



Response count 350

Threats Facing MSPs

AI Remains the Top Concern for MSPs

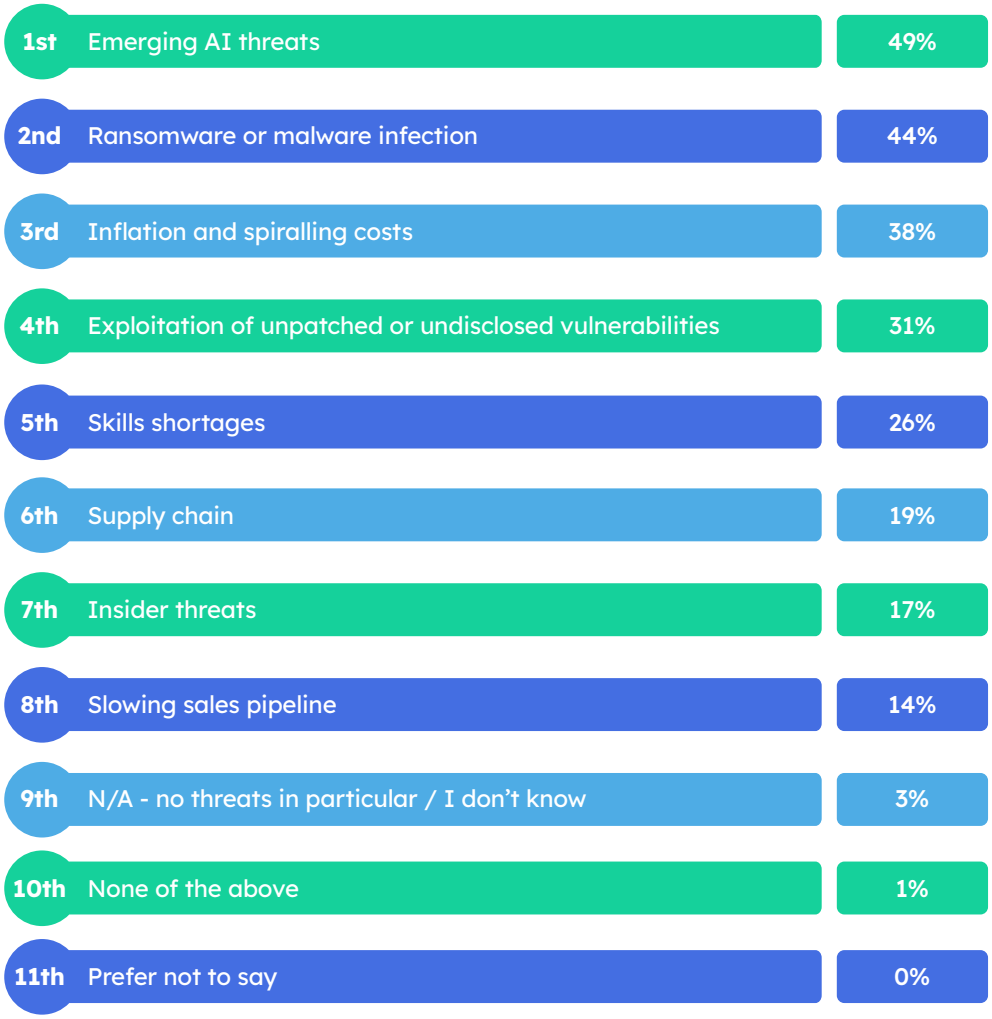
A 2026 UK government study found that AI usage has become widespread, with 73% of the public admitting to using it as part of their day-to-day lives. As AI tools become increasingly ingrained in our personal and professional lives, cybercriminals continue to find new ways to exploit them for malicious purposes.

It's unsurprising that emerging AI threats remain the leading concern for MSPs, named by nearly half (49%). It placed as the top concern for MSPs last year too.

While MSPs are well-versed in both traditional and emerging cyber threats, they are comparatively less equipped to address those posed by AI. The pace at which AI-driven threats evolve often outstrips the development of effective tools and guidance, leaving a noticeable gap between risk and response capability.

In April 2026, the NCSC, as well as senior ministers from the Department of Science, Innovation and Technology (DSIT), wrote a series of open letters about how British businesses can retain "defensive advantage in the age of frontier AI cyber capabilities". Richard Horne, CEO of the NCSC, said that "organisations must raise their security baseline to safeguard their cybersecurity". In these times, many SMEs will turn to MSPs for increased support in combatting the threat of AI.

Which, if any, of the following represents the biggest threats to the business you work for? [select up to three]



Response count 350

Other Top Concerns: Inflation and Supply Chain Risk

Inflation and spiralling costs have jumped from 5th to 3rd place this year, pushing insider threats to 7th. Geopolitical instability may be a contributing factor to this, given its widespread impact on inflation, energy prices and overall economic uncertainty.

Additionally, supply chain risk has risen from 7th (15%) to 6th (19%) among MSPs' top concerns. This shift likely reflects the growing focus introduced by the Cyber Security and Resilience Bill, which places greater scrutiny on MSPs' roles within the supply chain and is prompting many to reassess their position and responsibilities.

This rise in concern may also be driven by a series of high-profile supply chain breaches over the past year, as noted earlier. But more on the supply chain later...

Inflation and Costs are Critical Concerns for Customers

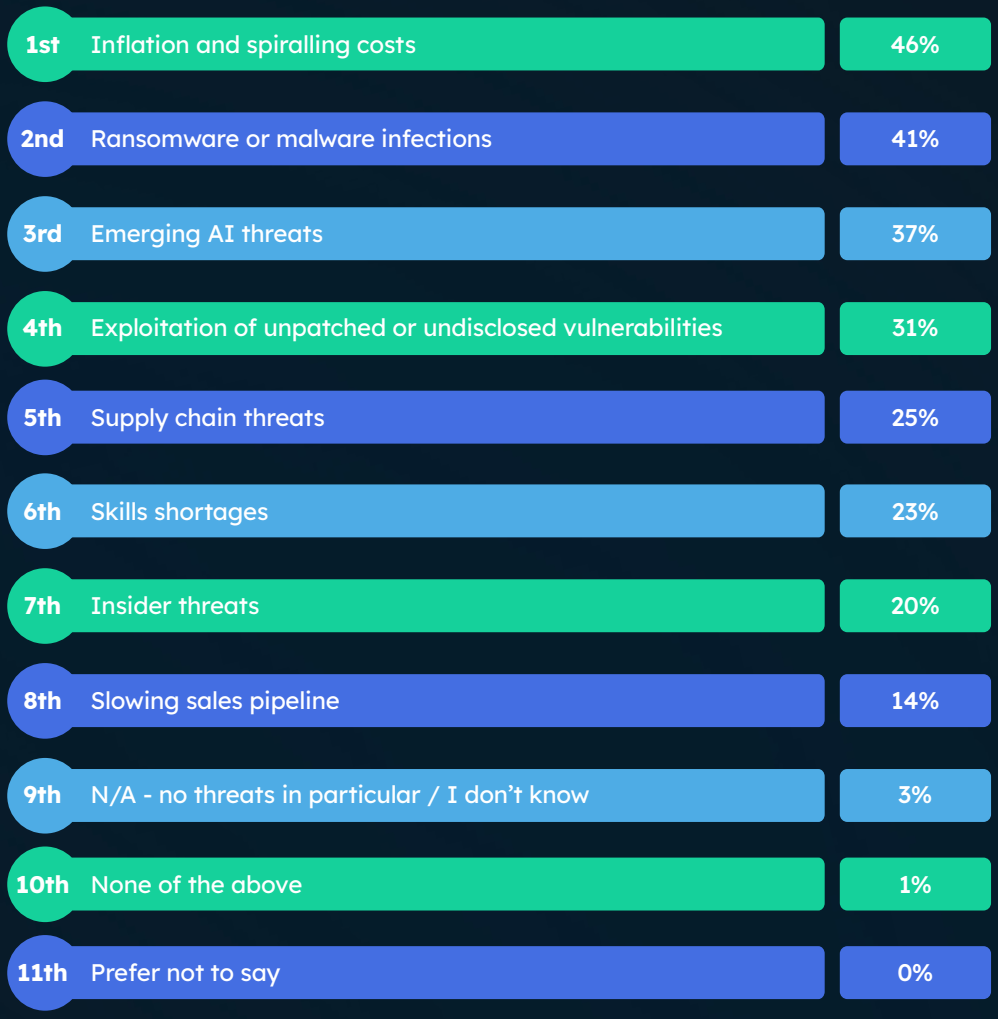
Whereas emerging AI threats remain the leading concern for MSPs, customers, who ranked them top of the list last year, have moved them to third. The threat hasn't changed, yet MSPs have spent a year helping clients get a working grip on it and the fear has come down accordingly. The risk when it comes to confidence is that the threat may drop off the board agenda and, in turn, the budget.

In 2026, the top perceived threats for customers are operational, as opposed to purely cyber or technical, with inflation and spiralling costs (46%) outranking traditional security concerns. In 2025, this ranked 5th (29%). This suggests that for many organisations, day-to-day business pressures and financial stability are taking precedence over emerging or even established cyber threats. This highlights that business resilience is currently being shaped as much by economic conditions as by the cyber threat landscape.

It also points to a broader challenge: in a strained economic climate, SMEs may struggle to absorb the cost of improving cyber resilience, particularly within supply chains, where expectations are rising. This raises important questions around responsibility and support, like who ultimately shoulders the burden of becoming more secure and whether greater use of incentives, such as tax breaks or subsidies, could help ensure that essential security investments are not deprioritised.

Similarly, it's worth noting that supply chain threats rose from 7th place last year (20%) to 5th place this year (25%). This is likely due to increased awareness of the topic, perhaps as a result of headline incidents and changing regulatory scrutiny.

Which, if any, of the following represents the biggest threats to your customers' businesses? [select up to three]



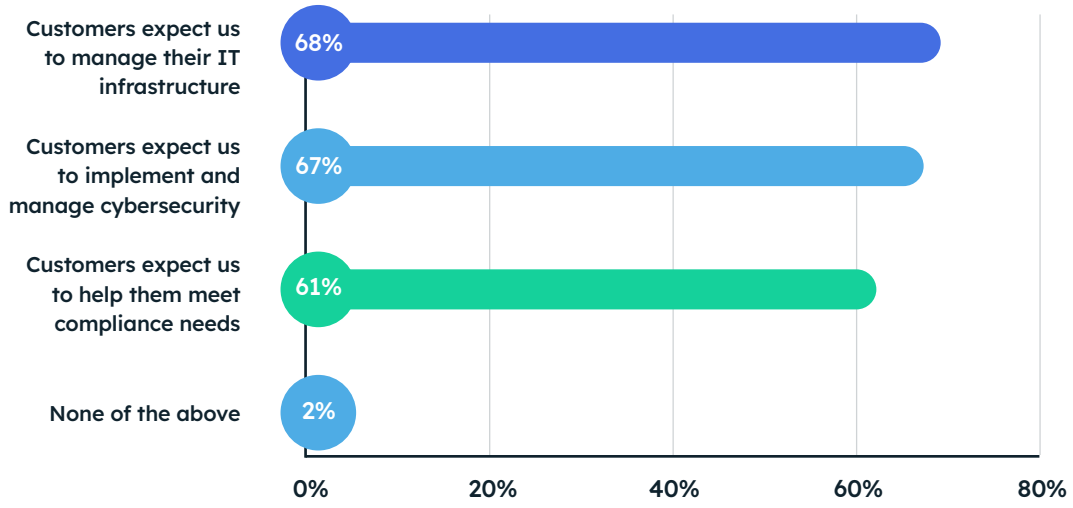
Response count 350

The Roles and Responsibilities of MSPs Continue to Change

Over the past few years, the role of the MSP has changed when it comes to customer expectations. In 2026, over two thirds of respondents noted that their customers expect them to manage both their IT infrastructure and cybersecurity (up from 60% in 2025). 61% of MSPs are expected to help their customers meet their compliance needs, too.

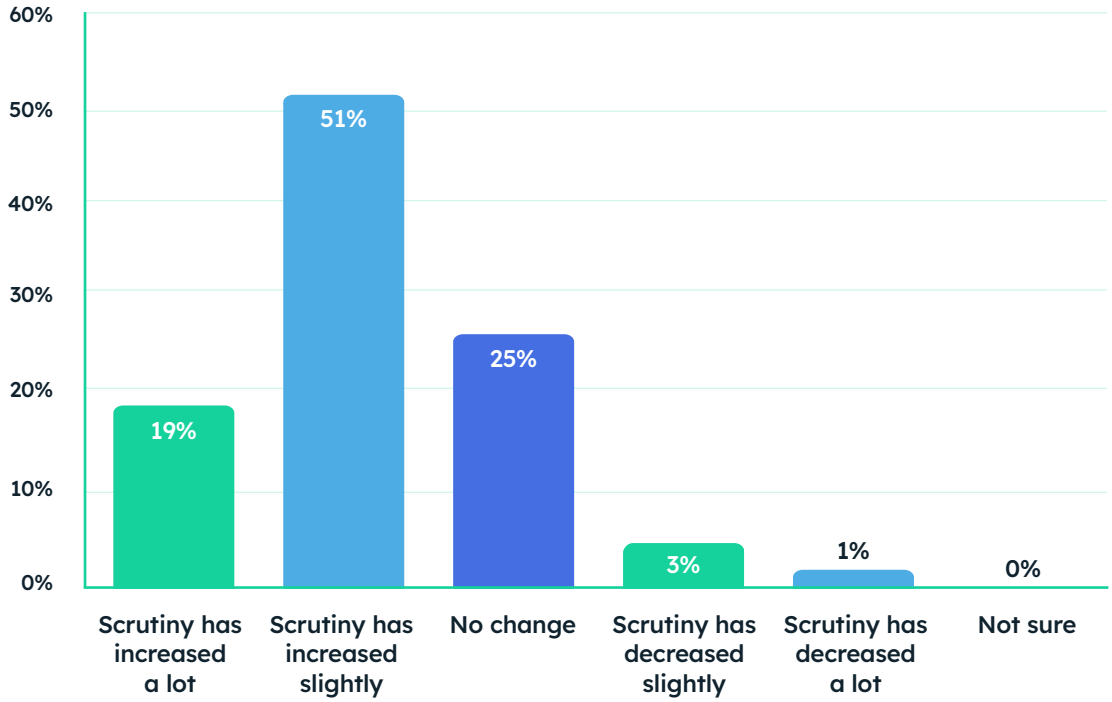
This is unsurprising given that regulations are changing in favour of keeping companies accountable for a continuous commitment to security. New changes to Cyber Essentials, for example, include the introduction of three auto-fail sections, as well as marked leadership accountability. This means that compliance must move beyond a tick-box exercise to a continuous year-round activity. Many organisations, especially SMEs, will turn to MSPs to help them meet and maintain these standards.

Which, if any, of the following do your customers expect from your services? [select up to three]



Response count **900**

Have you noticed a change in the amount of scrutiny placed on your business' security capabilities during new RFP (Request for Proposal) /New business meetings in the last 12 months?



Response count 350

Scrutiny on MSPs Has Eased

The share of MSPs reporting rising scrutiny has eased from 77% in 2025 to 70% in 2026. This reads less like a loss of interest and more like customers no longer being surprised by what they see.

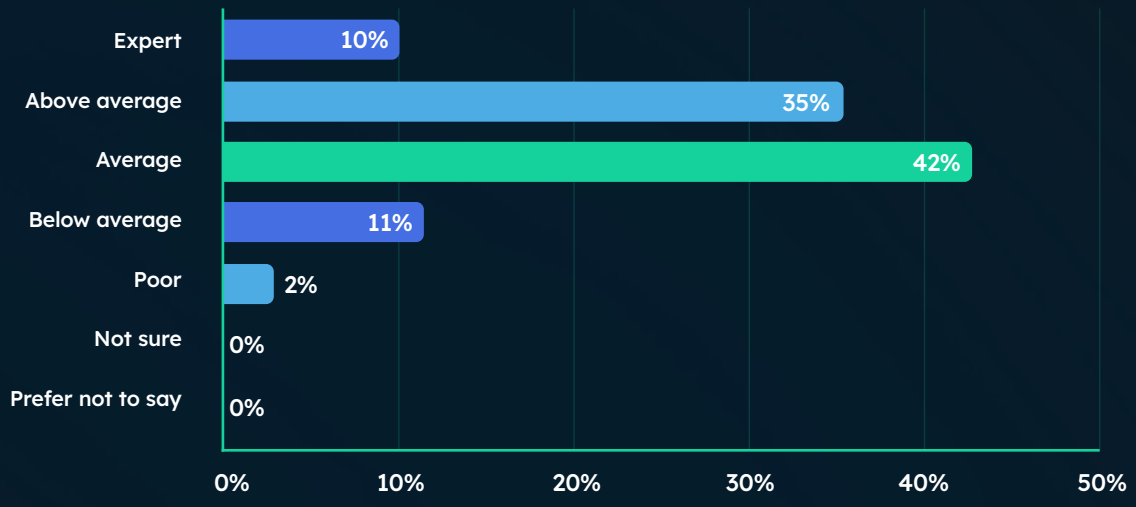
As security expectations become more standardised and better understood, scrutiny is shifting from reactive questioning to a more established, ongoing part of vendor evaluation. In other words, rather than intensifying year-on-year, scrutiny may now be stabilising as a baseline requirement embedded in procurement, compliance and day-to-day oversight, rather than being driven by spikes in concern.

Customer Maturity

The 2026 survey suggests that customers have matured in their understanding of cybersecurity. In fact, most (87%) are now rated by their MSPs as having average or above average cyber knowledge.

Evidently, these organisations recognise the risks they face and are actively seeking MSP support to help protect their businesses. Trust and understanding between MSPs and customers go both ways.

How would you describe the cybersecurity knowledge of your average customer?



Response count 350

Investment in Evolution Towards Managed Compliance Services

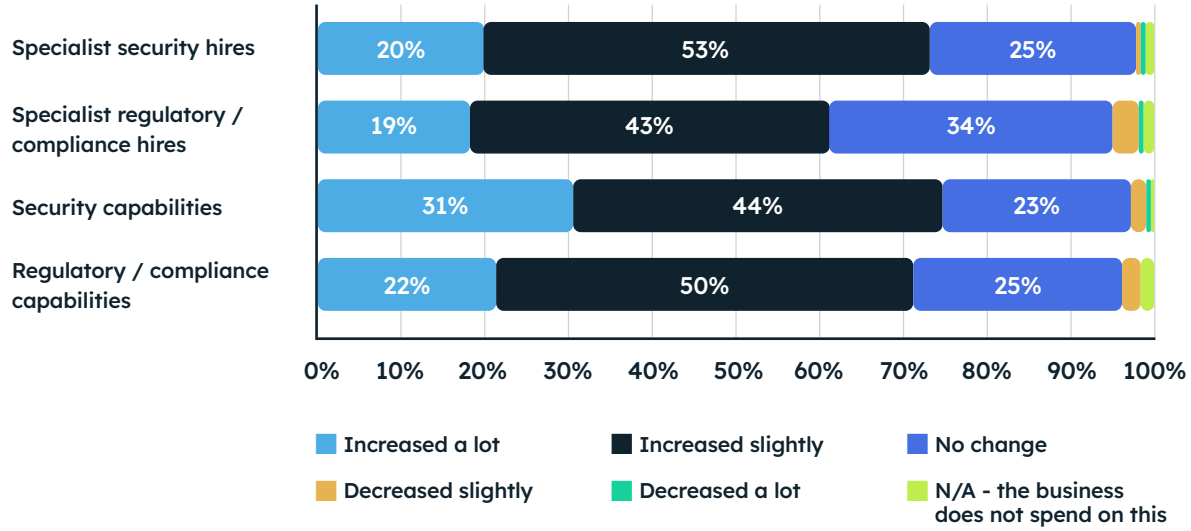
Increased spending on regulation and compliance has risen from 64% to 72% over the past year. The commitment is clearly there, yet many MSPs would benefit from a clearer, more consistent target, with defined baseline standards, a clearer depiction of responsibilities and more practical guidance on how to operationalise and demonstrate compliance.

This likely reflects growing regulatory pressure, potentially linked to developments such as the Cyber Security Resilience Bill, as MSPs look to get ahead on compliance. It also aligns with broader customer and market expectations to demonstrate stronger security and governance.

Looking ahead, MSPs' top areas for investment over the next one to three years - training (51%), continuous monitoring (46%) and proactive risk management (44%) - reinforce this shift. These priorities point to a more mature, ongoing approach to security and compliance, rather than one-off controls. Even areas like incident response planning (ranked 6th) play a role in demonstrating compliance readiness.

Together, this highlights a broader market evolution: MSPs are moving beyond traditional security provision and increasingly positioning themselves as providers of managed compliance services too.

How, if at all, has your business' spend in each of the following areas changed over the past 12 months?



Response count 350

Which, if any, of the following areas do you expect will be the main focus for investment and growth over the next 1 to 3 years for the business you work for? [select all that apply]

Response count 350

Navigating Supply Chain Cybersecurity

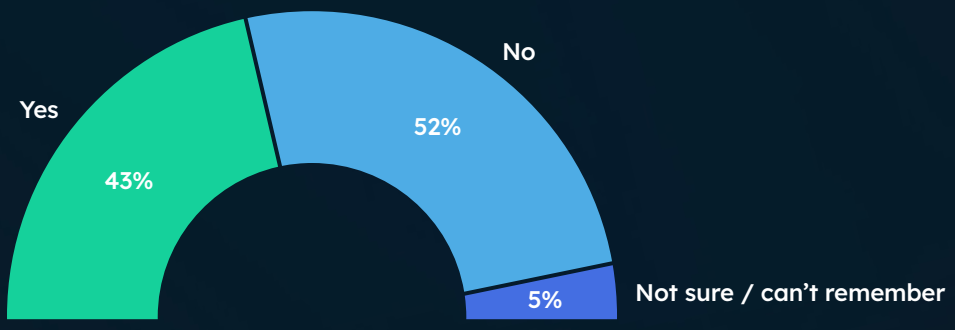
Third Party Risk is Now Mainstream

Over the past year, it has become clear that supply chain breaches are systemic, not incidental. **One attack on a major British retailer**, which is thought to have cost the organisation around £300m, occurred as a result of third-party access into its systems via a supplier. **Another notable cyberattack on a British car manufacturer** is believed to have had an estimated £1.9bn economic impact and a significant ripple effect across ~5,000 suppliers and partner organisations. These are just two examples of the many high-profile incidents that have hit British institutions this year. What's clear is that third parties are fast becoming a coveted primary entry point and that knock-on operational disruption is the real impact.

MSPs are uniquely situated in the supply chain, as they often have privileged access to the inner workings of their customers' organisations. This makes them a highly coveted target for cybercriminals and the potential gateway to tens, if not hundreds, of other organisations.

The survey reveals a stark truth: two in five MSPs, or their customers, have experienced a cyber incident caused by or originating from a supplier or third-party vendor in the past 12 months. Evidently, third-party risk is clearly mainstream.

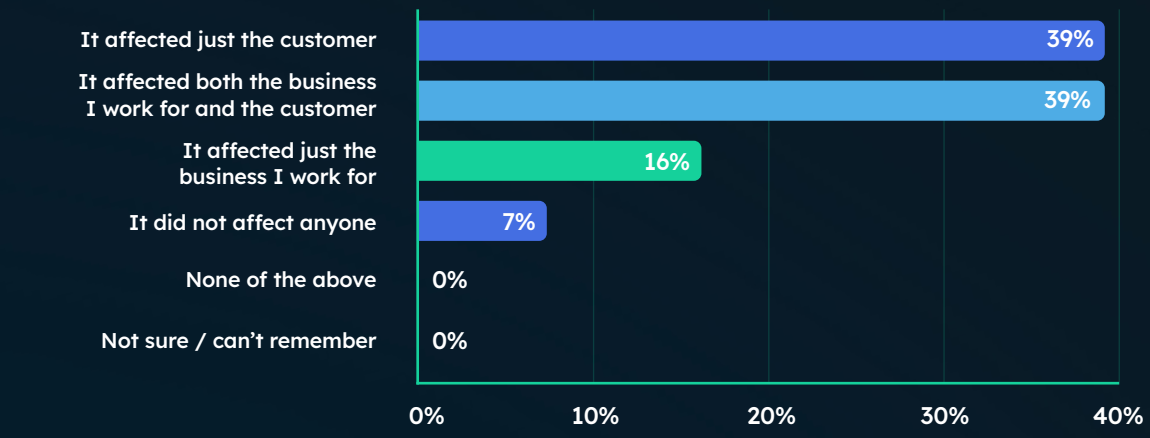
Has the business you work for or any of your customers experienced a cyber incident caused by or originating from a supplier or third-party vendor in the past 12 months?



Response count 350

Of those who experienced a supply chain incident, 39% were affected only by the customer, 16% only by the MSP, and 39% by both the MSP and the customer. This means that over half (55%) of incidents involve the MSP in some way. This suggests incidents rarely stay contained, instead spreading across interconnected systems, where shared access and dependencies allow breaches to move between MSPs and customers.

Thinking about the most recent cyber incident that was caused by or originated from a supplier / third-party, who, if anyone, was affected by it? [select best match]



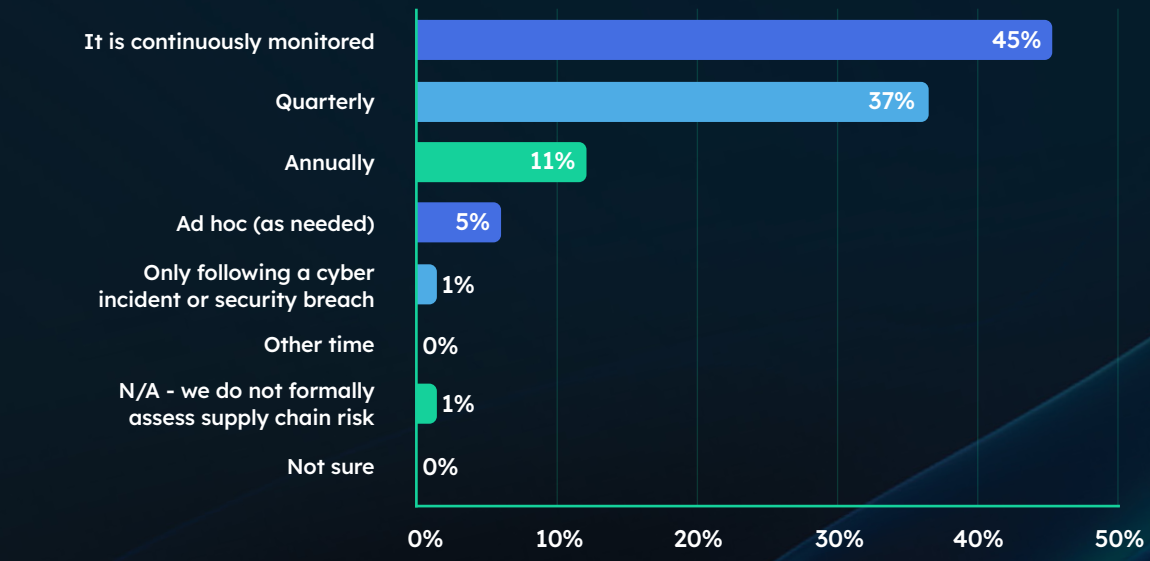
Response count 350

Monitoring Risk

Regulatory momentum is moving towards continuous monitoring and real-time risk visibility. More advanced standards, such as ISO 27001 (particularly Clauses 6.1 and 9.1), require organisations to maintain an ongoing cycle of risk assessment, monitoring and review. Additionally, updates to Cyber Essentials in April 2026 emphasise the importance of moving beyond point-in-time security, encouraging organisations to demonstrate ongoing adherence to cyber best practices and to take greater accountability at the leadership level.

Yet, the survey reveals that MSPs are a long way off this. Only 45% of the leaders surveyed say that their MSPs monitor third-party risk continuously. The rest - over half - rely on periodic reviews. This is a risky position given what MSPs are structurally: a supply chain to their customers, and one of their own.

When, if ever, do you typically assess/reassess your business' supply chain cyber risk? [select best match]

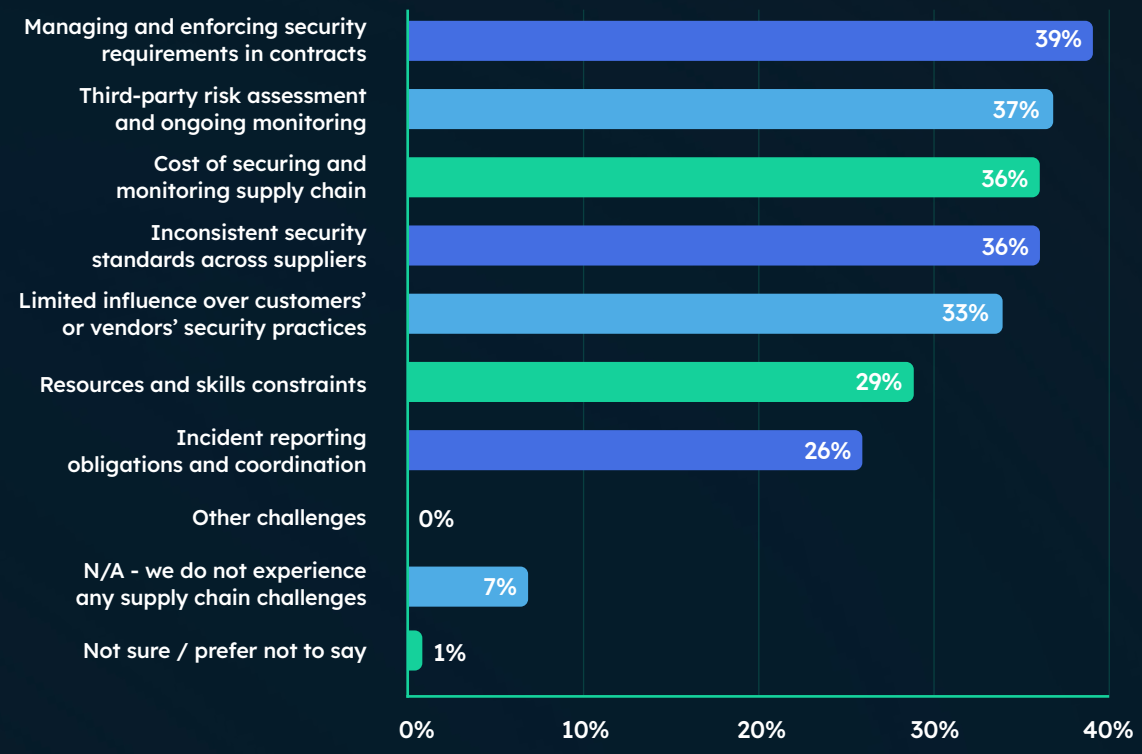


Response count 350

Governance, not technology

Ask MSPs what's hardest about securing the supply chain and the answers point away from tooling. Contract enforcement leads the list (39%), followed closely by third-party risk assessment (37%), cost of monitoring (36%) and inconsistent standards across suppliers (36%). Process, paperwork and negotiation, mostly.

What, if anything, are the biggest challenges when it comes to securing your customers as part of the supply chain? [select up to three]



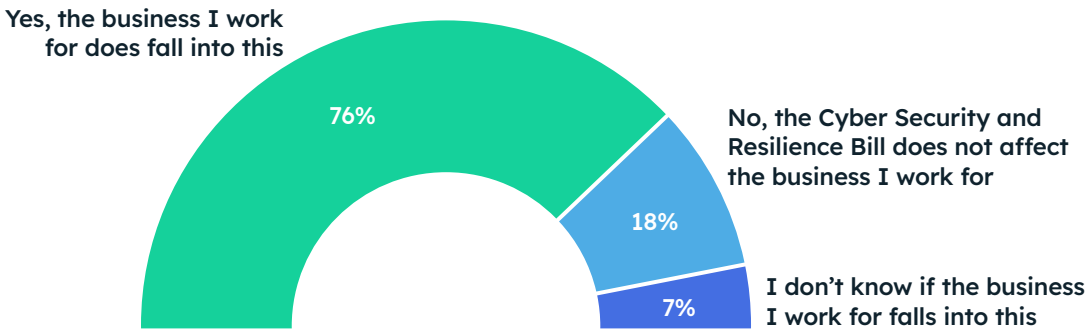
Response count 350

The Cyber Security and Resilience Bill

The Cyber Security and Resilience Bill, introduced in November 2025, brings MSPs into the scope of formal UK cyber regulation for the first time, introducing mandatory security requirements, stricter incident reporting and greater accountability. It reflects a broader shift towards managing systemic supply chain risk and positions MSPs not just as service providers, but as critical components of national cyber resilience.

Of those we surveyed, 76% said that their MSP falls into scope. Large and medium-sized MSPs that meet the definition of a 'Relevant Managed Service Provider' (RMSP) are expected to comply with the Bill. While this legislation is broadly aligned with NIS-style thresholds (typically organisations with 50+ employees and €10m+ turnover), the exact criteria will depend on how the legislation is finalised and applied in the UK. **DSIT research** suggests around 1,214 MSPs in the UK may fall into scope.

Do you know whether your MSP is covered by this Cyber Security and Resilience Bill (i.e. required to comply with its cybersecurity obligations)?

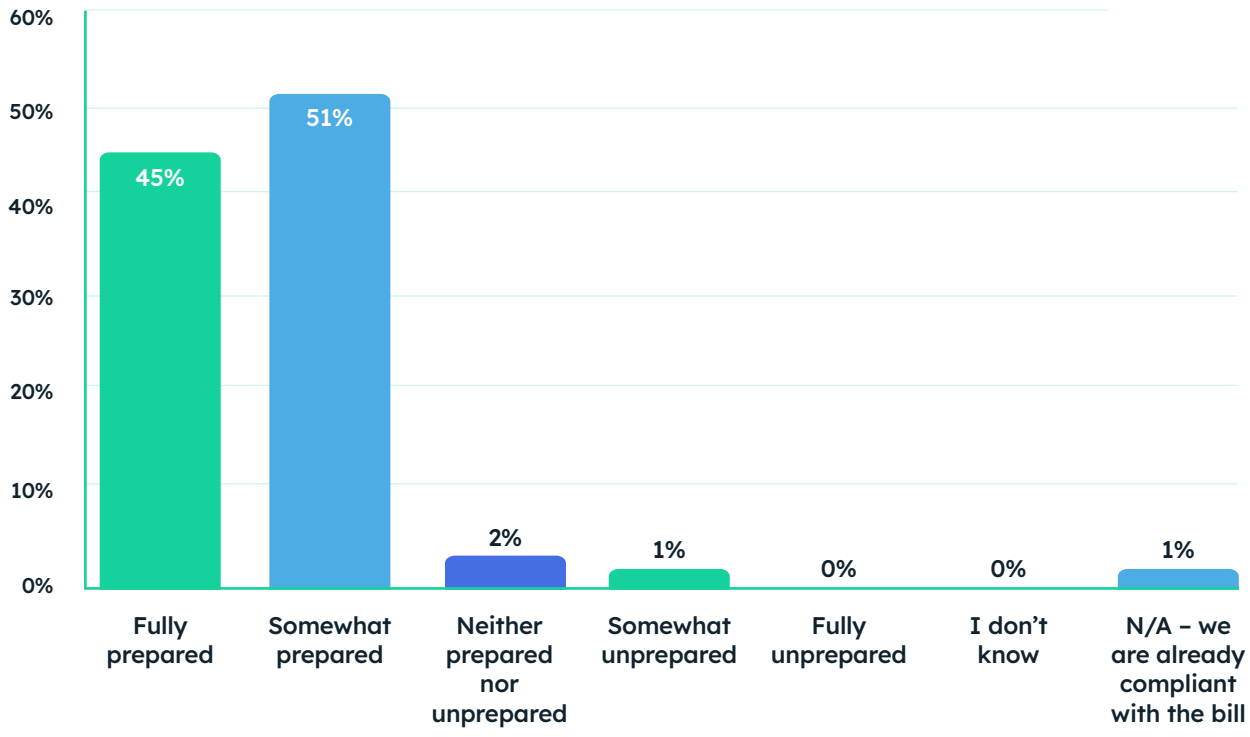


Response count **350**

Overall, the vast majority of those who fall into scope (96%) say that they are prepared to a certain extent, with 51% saying that they're 'somewhat' prepared and 45% saying that they're already 'fully' prepared. What's positive is that regulation is already influencing behaviour. The high preparedness figure suggests MSPs are already responding proactively to regulatory direction.

However, readiness remains a work in progress. These organisations have seemingly established a foundation but are likely still addressing gaps in capability, clarity and execution. Confidence is high, but full operational readiness is not yet universal.

How prepared or unprepared is your business to implement the changes required to comply with the Cyber Security and Resilience Bill?

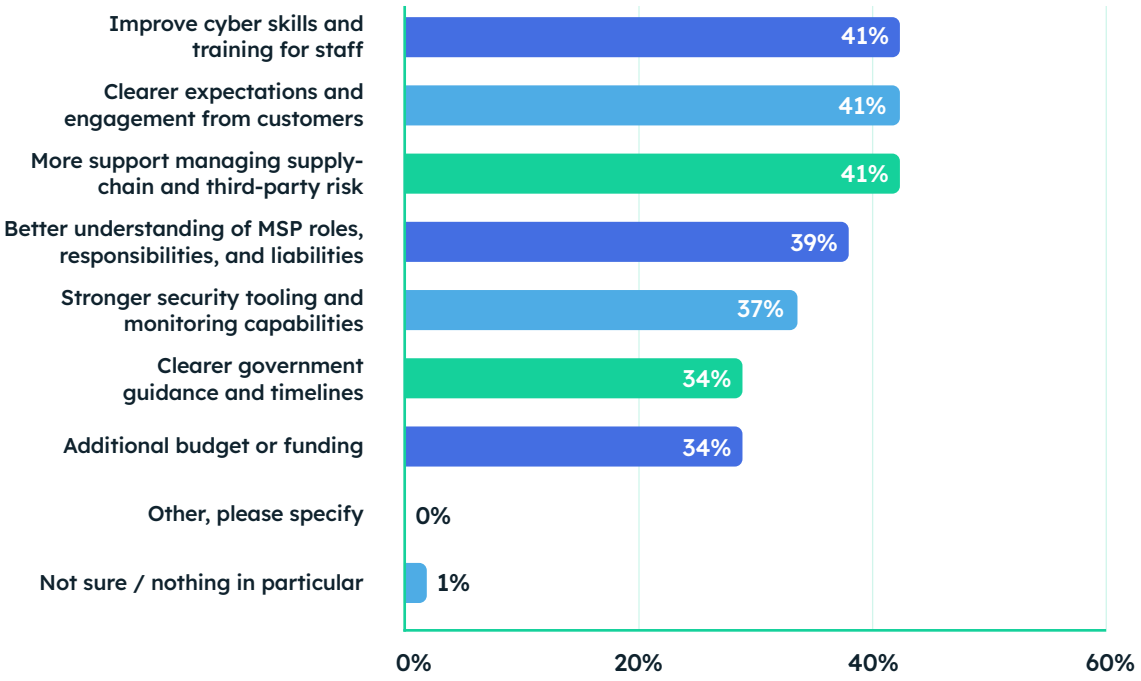


Response count 350

The Coordination Gap

Notably, MSPs do not see software as the solution to closing the readiness gap. Instead, they point to skills, clearer customer expectations, stronger support for managing third-party risk and better-defined roles and liability, each cited by around four in ten. This highlights that the challenge is less about technology and more about coordination, capability and clarity across the ecosystem.

What, if anything, would most help improve your business' readiness for The Cyber Security and Resilience Bill? [select up to three]



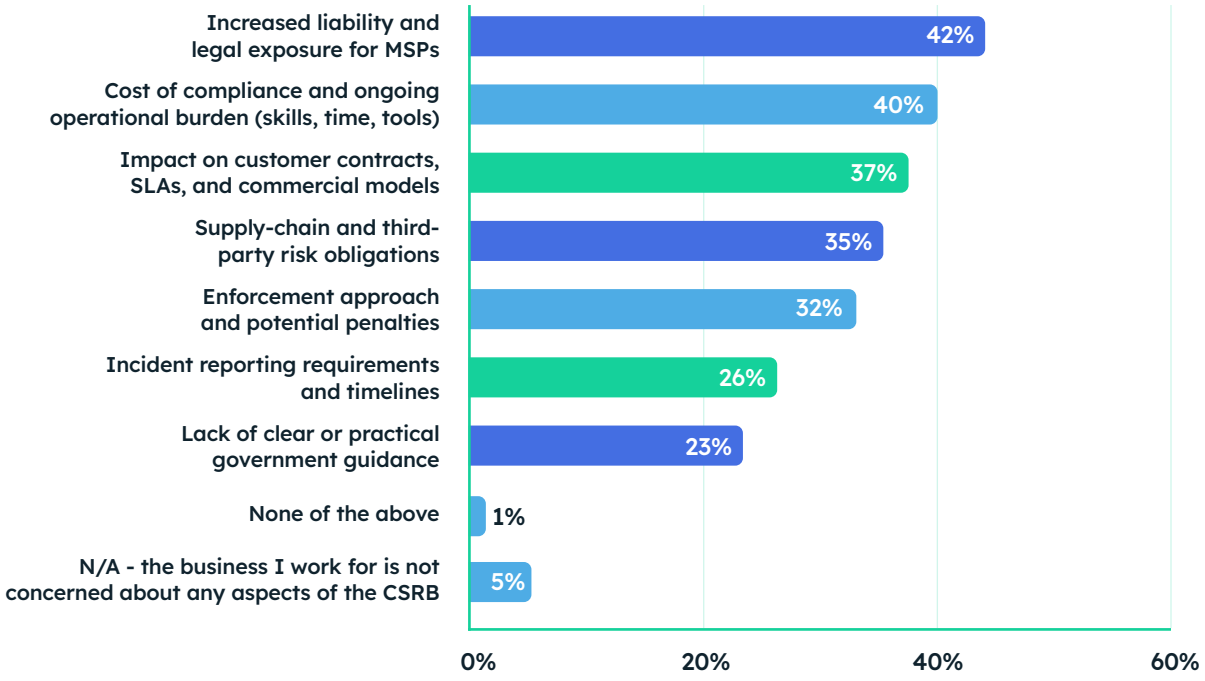
Response count 350

When it comes to concerns around the Cyber Security and Resilience Bill, MSP leaders are worried about undefined accountability, not about accountability itself.

The single biggest concern is increased liability and legal exposure (42%). The issue is being held to account without clear definitions of responsibility, especially when the consequences of non-compliance, whether for the individual or the organisation, can be costly.

With costs, contracts and guidance also ranking highly, MSPs are grappling less with the principle of regulation and more with how risk will be allocated and operationalised in practice.

Which, if any, of the following aspects of the Cyber Security and Resilience Bill (CSRB) is your business most concerned about? [select up to three]



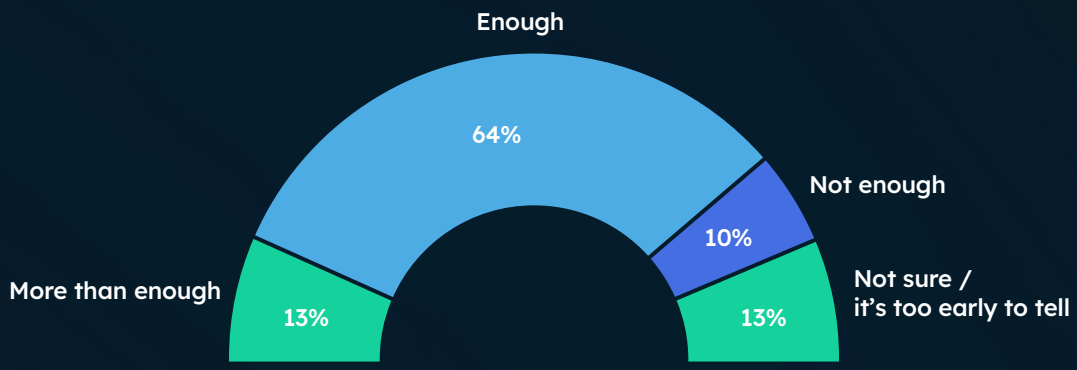
Response count 350

Futureproofing MSPs

The Cyber Security and Resilience Bill is broadly welcomed, with more than three-quarters of MSPs stating that they believe it's doing enough. What the industry wants isn't less regulation, but clearer regulation: better guidance, stronger liability protections, frameworks that reflect how MSPs actually work, each named by roughly half of respondents.

This points to a broader theme of futureproofing. MSPs are not resisting change. Evidently, they're preparing for it. Clearer, more practical regulation would enable them to build scalable, repeatable security and compliance models, rather than navigating ambiguity on a case-by-case basis. In this sense, futureproofing is about making regulation actionable by giving MSPs the clarity needed to invest with confidence, define responsibilities and embed resilience into their services over the long term.

Do you think the Cyber Security and Resilience Bill is doing enough in protecting supply-chain organisations, including MSPs, from cyber risk?



Response count **350**

Which, if any, of the following do you think should be done more to protect MSPs from cyber risk in general? [select all that apply]

Response count 350

Key Takeaways

Finally, what can we learn from the survey results? Here are our key takeaways:

1. Breach frequency has eased compared with last year, but not enough to change the picture significantly: more than half (54%) of MSPs were breached twice or more in the past 12 months. Repeat breaches are still too commonplace for comfort.
2. Inflation has climbed into MSPs' top three concerns and sits at the top of their customers' list at 46%, up from fewer than three in ten a year ago. This suggests that cyber risk has merged with the economy; you can't plan one without reference to the other.
3. Emerging AI threats remain the leading concern for MSPs, named by nearly half. Customers who had them at the top of the list last year have moved them to third place. This suggests that customers are feeling more supported in tackling these threats.
4. Increased spending on regulation and compliance has risen from 64% to 72% over the past year. The commitment is there, yet a clearer target would help. Additionally, 61% expect their MSP to help them meet compliance obligations.
5. Customers have matured. Most are now rated by their MSPs as having average or above cyber knowledge.
6. The share of MSPs reporting rising scrutiny has eased from 77% to 70%, which reads less like a loss of interest and more like customers no longer being surprised by what they see.
7. Two in five MSPs or their customers were hit by a supplier-originated incident this year. In more than half of those cases, the MSP was caught up in it alongside the customer. This exemplifies how supply chain incidents can travel.
8. Only 45% of MSPs monitor third-party risk continuously. The rest rely on periodic reviews, which potentially leaves risky gaps.
9. Ask MSPs what's hardest about securing the supply chain and the answers point away from tooling. Contract enforcement leads the list, followed closely by third-party risk assessment, cost of monitoring and inconsistent standards across suppliers.
10. The Cyber Security and Resilience Bill is broadly welcomed. More than three-quarters of MSPs think it's doing enough. What the industry wants isn't less regulation, but clearer regulation.
11. The single biggest concern about the Cyber Security and Resilience Bill is increased liability and legal exposure at 42%. The worry isn't being held to account. It's being held to account for something nobody has yet defined.
12. Almost all MSPs say they're prepared for the Cyber Security Resilience Bill to some degree. Fewer than half say they are fully prepared (45%). When asked what would close the gap, the top answers are about clarity and capability, rather than tooling:
    a. Skills (41%)
    b. Clearer customer expectations (41%)
    c. Better support on third-party risk (41%)
    d. Clearer understanding of MSP roles and liability (34%)


CyberSmart
cybersmart.co.uk