CyberSmart

The CyberSmart MSP Survey 2025

Introduction

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

As of 2024, it's estimated that in the UK, **11,492 active MSPs** generate around £52.6 billion in annual revenue and employ some 294,000 people. It's a similar story in the rest of Europe, with MSPs projected to be **worth €234.2 billion** to the EU economy by 2026.

However, MSPs' importance to the global economy goes far beyond their revenue generation. For many businesses, particularly SMEs, MSPs represent a one-stop shop for their IT needs. MSPs provide and administer everything from office software packages to network security and **cyber awareness training**, making them the critical node in most supply chains.

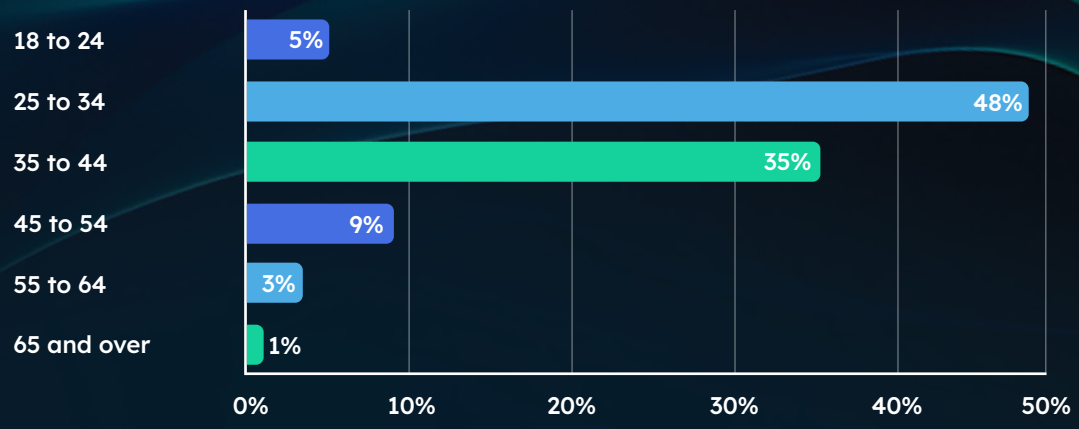
Unfortunately, the very things that make MSPs so important also draw the attention of cybercriminals. As trusted partners to millions of businesses across the globe, MSPs typically have access to clients' infrastructure and inner workings. This renders them a highly lucrative target, whether for their own data or their clients'. Indeed, **60% of MSPs** we surveyed last year felt their clients were more at risk in the past 12 months than previously.

Yet, for all their importance, MSPs are often overlooked. You'll rarely hear about them in the media, and beyond the odd government report, there's little research conducted about these organisations that form the backbone of many economies. And this is especially true when it comes to their cybersecurity.

In 2024, we set out to change this with our **first MSP survey**. For 2025, we've teamed up again with One Poll to ask MSPs some key questions about their cybersecurity. How well defended are they? What do they feel are the biggest threats facing them and their customers? And, with cybersecurity legislation on the horizon across the globe, how are they preparing?

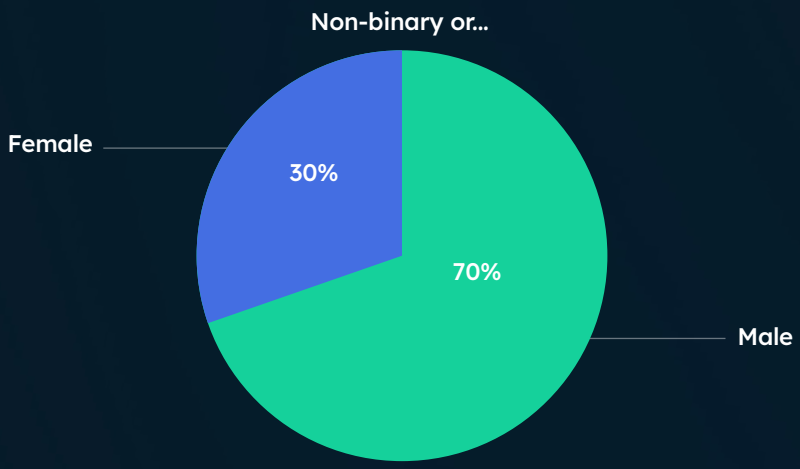
To ensure we're getting the most complete picture possible, this year we've expanded the survey to include markets with a strong MSP presence across the globe. The 2025 edition features 900 MSP leaders from the UK, France, Belgium, Australia, New Zealand, Sweden, Germany, and the Netherlands, with customers of varying sizes from 1 to 250+ employees.

What is your age?



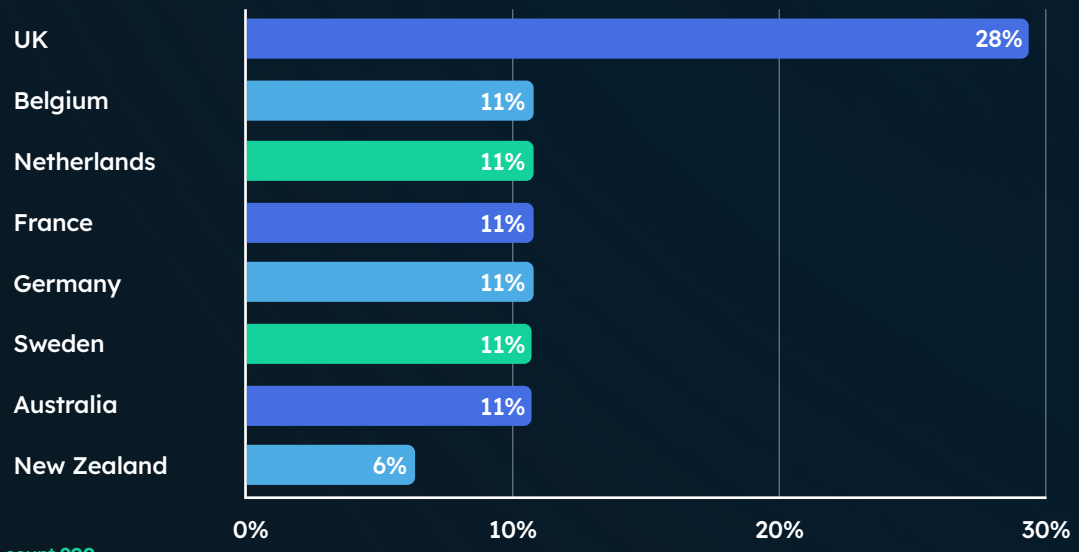
Response count 900

Are you...?



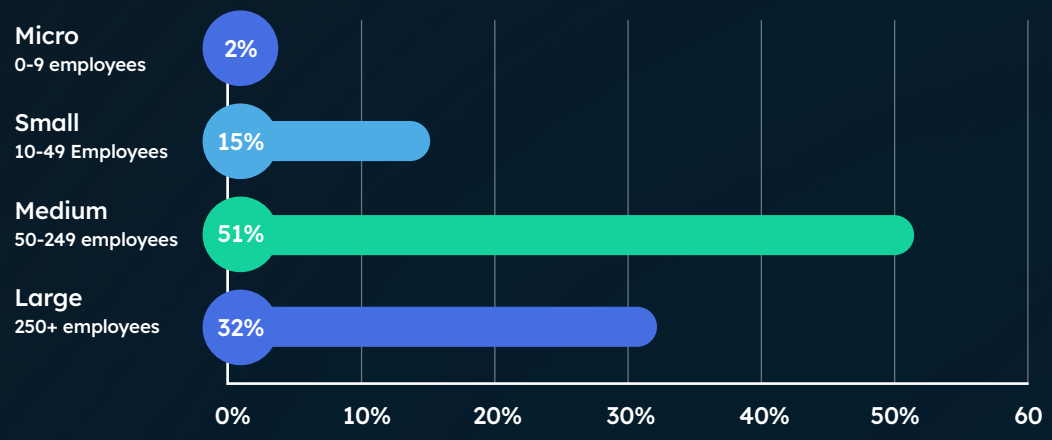
Response count 900

Where to you live?



Response count 900

What most accurately describes the average company size of your customers? [select one]



Response count **900**

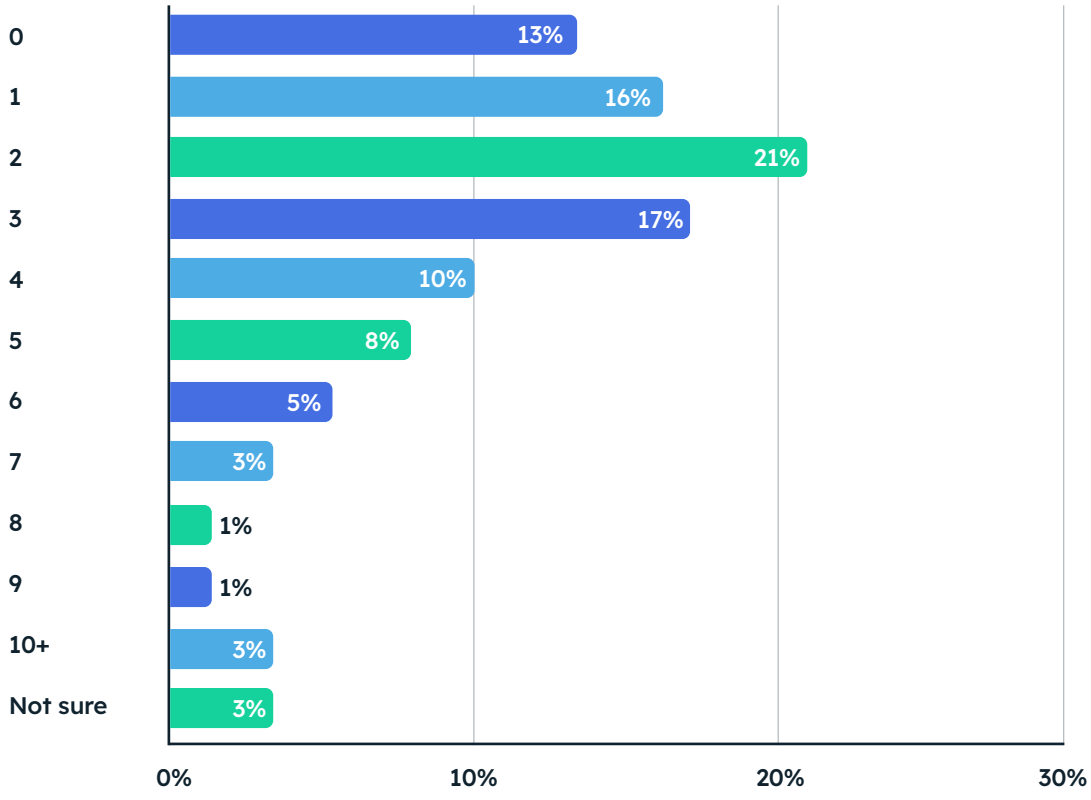
What follows are the results of this study, providing an accurate picture of the cybersecurity landscape for MSPs and their customers in 2025.

MSPs are being breached at an alarming rate

The last year has seen a number of high-profile breaches of MSPs. One such example is the **£3m fine levied by the Information Commissioner's Office** (ICO) on an MSP providing software and services to the NHS in March 2025, over security failings that led to a ransomware attack.

Or, even more recently, in May 2025, the Dragonforce ransomware gang **breached an MSP's remote monitoring and management (RMM)** tool in order to conduct a supply chain attack. But beyond the headlines, our survey uncovered evidence that breaches of MSPs are widespread.

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



Response count 900

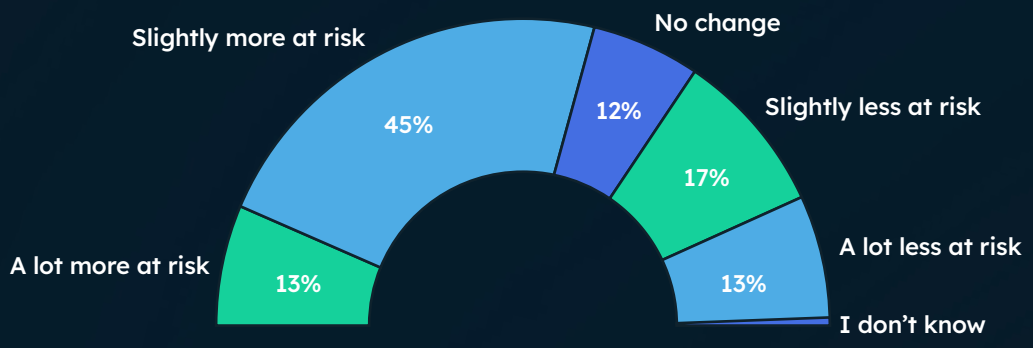
Of the 900 MSP leaders we surveyed, 69% reported being breached two or more times in the last 12 months. This represents a slight increase from the 67% who reported breaches in our 2024 edition. Shockingly, 47% of those surveyed had experienced three or more breaches in the last 12 months.

Of course, there is a caveat. A "breach" can mean anything from a minor incursion to business-critical data or systems being compromised, and many of the incidents reported are likely to be the former. However, breaches at MSPs remain far too high for comfort.

Most MSPs feel their customers are more at risk in the last 12 months than they were previously

2025 has become the year of the major cyber breach. We've seen everyone from **big-name retailers** to **government agencies** being hit with attacks. So it's not a surprise to see that MSP leaders are about as concerned for their customers' cyber safety as they were in 2024.

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



Response count **900**

Indeed, 58% of those that we surveyed felt their customers were more at risk, a slight decrease from 61% last year. However, what is interesting is that the percentage of MSPs who sense no change in risk level over the last 12 months has halved (from 24% to 12%).

This suggests that MSPs broadly fall into two camps on risk. Either they're relatively confident in their customers' cybersecurity measures, and so feel risk has declined, or emerging threats have made them more concerned than ever.

We'll dig into the former later in the report, but let's tackle emerging threats next.

Emerging AI threats are what keep MSP leaders up at night

Earlier this year, Forbes labelled 2024 "**a landmark year in the evolution of AI**", and in many ways it was. 2024 was the year many of us began using generative AI in our day-to-day lives and work. However, as with any new technology, the rise of generative AI has a darker side. Cybercriminals, never ones to miss a chance at innovation, have also begun using the technology, whether for uber-convincing deepfakes, spinning up malware in minutes, or **weaponising AI's tendency to hallucinate** to launch attacks.

It's perhaps this which explains why AI has rocketed to the top of MSP leaders' concerns. Some 44% of our respondents listed it as a concern, which is remarkable when you consider that it barely featured in last year's report. Worryingly, it's also probably the threat most MSPs are least well-equipped to deal with, due to the lack of easy-to-use tools to counter AI-powered attacks.

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

Response count **900**

Elsewhere, it's unsurprising that MSPs remain very concerned about ransomware and malware (40%), given the prevalence of both in the news cycle and **figures released by the Department for Innovation, Science & Technology (DSIT) earlier this year**, indicating a rise in incidents. Likewise, **83% of organisations reported experiencing an insider threat** in 2024, so it's not a shock to see it on 40% of MSPs' radars.

There's also a clear understanding from MSPs about the dangers unpatched vulnerabilities pose to their business, with 31% listing it as a top concern.

One area that is surprising is how few respondents (15%) listed **supply chain attacks** as a major concern. Due to the nature of their business, MSPs are one of the most at-risk sectors for this kind of attack. In fact, it's often the reason cybercriminals target them in the first place, whether to gain access to a bigger customer or the MSP's wider network.

How about the threats facing MSPs' customers?

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

Response count 900

It's a similar story when it comes to what MSPs feel is most threatening to their customers. Emerging AI threats (38%), ransomware or malware (38%), insider threats (35%), and unpatched vulnerabilities (32%) lead the way.

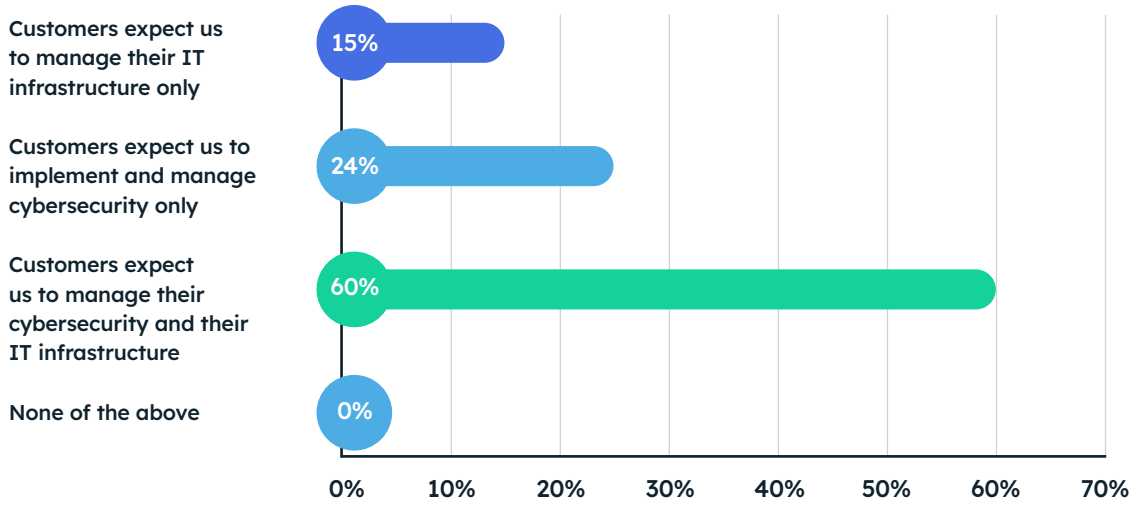
Once again, the headline is the emergence of AI as the threat MSPs feel is the biggest to their clients' businesses. By comparison, 2024's results skewed much more heavily towards malware and ransomware (55%) and inflation and spiralling costs (43%).

This doesn't mean MSPs aren't concerned about the economic outlook or ransomware, far from it. MSPs still rate both highly in their list of concerns (particularly ransomware at 38%). Nevertheless, it appears that AI is considered a threat so existential that it supersedes everything else in 2025.

MSPs are broadening to become cybersecurity providers

In last year's report, we highlighted how customers increasingly expect MSPs to manage and implement their cybersecurity alongside IT services. In 2024, 65% of MSP leaders we spoke to told us that customers now expect them to manage their cybersecurity.

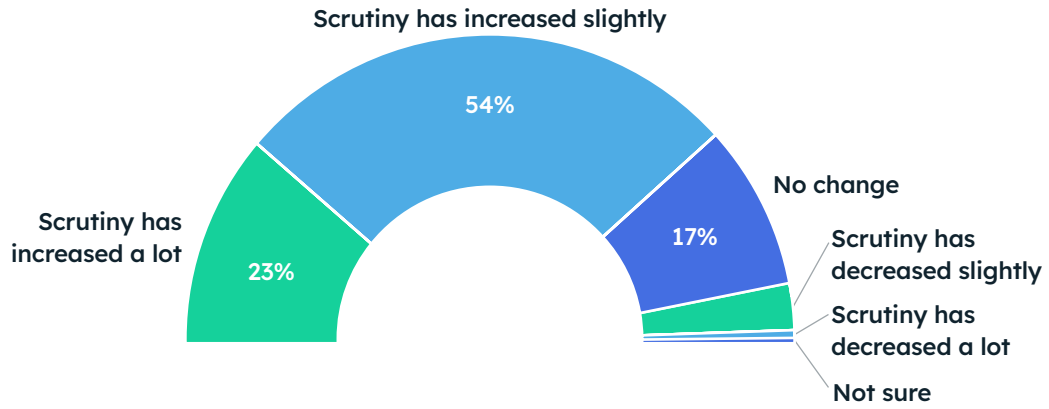
5. Which of the following best describes your customers' expectations of your services?



Response count 900

This trend has continued in 2025. A staggering 84% of MSPs now manage either their clients' cybersecurity infrastructure or their clients' cybersecurity and IT estate combined.

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

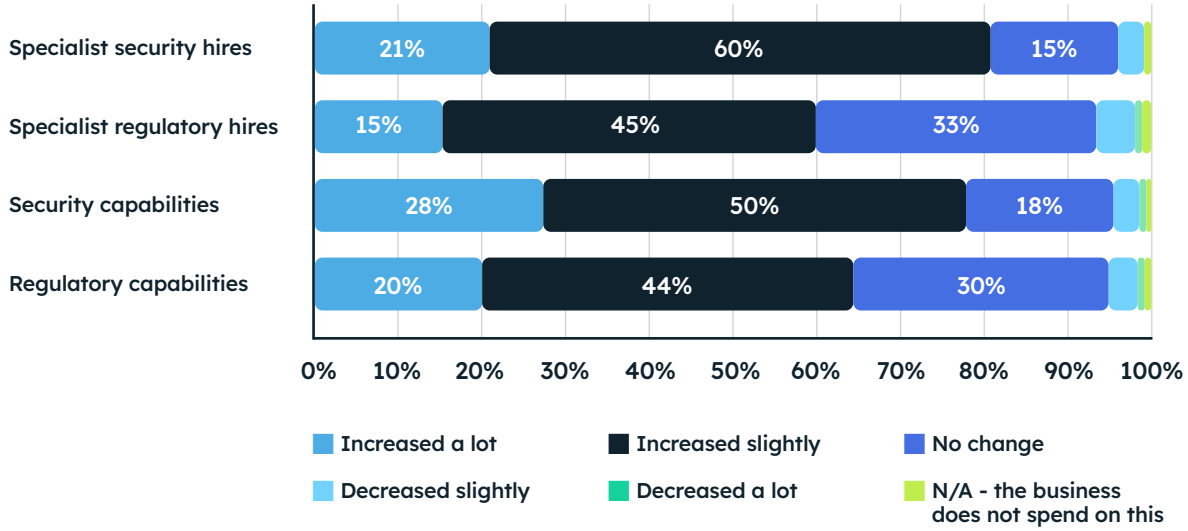


Response count **900**

This growing expectation for MSPs to manage cybersecurity is reflected in the scrutiny placed on them by customers in new business meetings. 77% of respondents said scrutiny of their businesses' security capabilities has increased either slightly or a lot, suggesting that MSP customers are more aware than ever of the importance of good cyber credentials in a potential partner.

There's also evidence that MSPs are retooling or expanding their cybersecurity operations to meet demand.

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



Response count 900

81% of the MSPs we spoke to said they'd increased spend on specialist cybersecurity hires. Likewise, 78% had upped spending on their security capabilities such as training, defences or products and services for customers.

But it's not just security that MSPs have invested heavily in over the past 12 months.

As we'll see later in this report, MSPs are increasingly concerned about compliance with cybersecurity regulations. Whether it's the European Union's **Network and Information Systems Directive 2** (NIS2), **Essential 8** in Australia, or the UK's upcoming **Cyber Security and Resilience Bill**, compliance with regulations has become an important part of the landscape for MSPS across the globe.

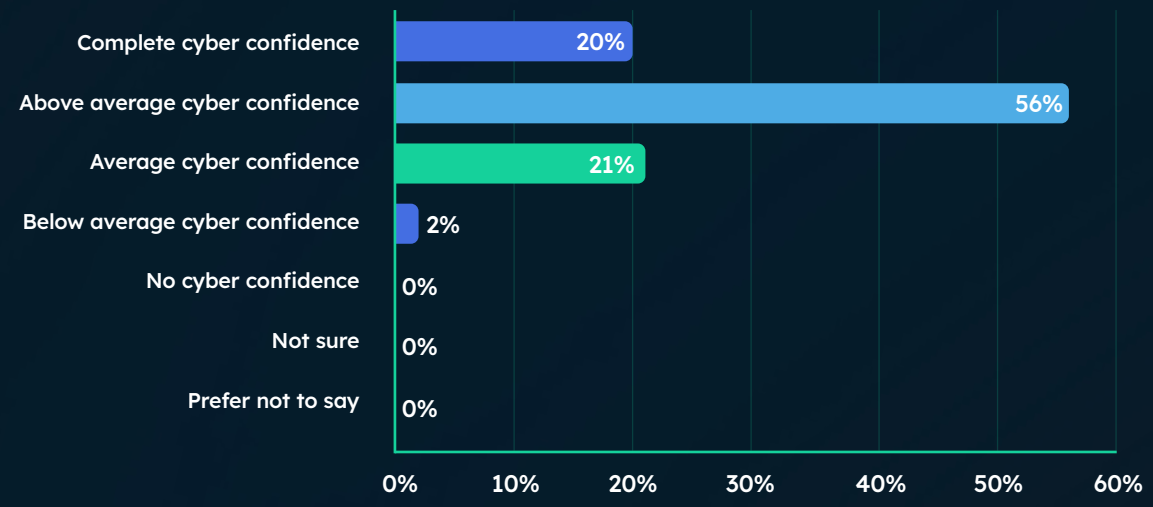
As a result, MSPs are spending big on regulation. 60% of our respondents had invested in specialist regulatory hires in the last 12 months. Meanwhile, 64% had increased spending on regulatory capabilities over the same period.

MSPs remain confident despite high breach levels

As we mentioned in the first section of this report, the number of MSPs reporting multiple breaches in the last 12 months is alarmingly high. Nevertheless, this doesn't seem to have dented MSP leaders' confidence in their organisations' cybersecurity.

76% of respondents said that their business displayed either complete or above average cyber confidence, despite 69% of them suffering multiple breaches in the past year.

8. At what level would you categorise your business' cyber confidence? [Cyber confidence is the overall level of trust and assurance an organisation has in their ability to protect data, digital assets, and systems from cyber threats]



Response count **900**

However, before we conclude that MSPs are overconfident in their cybersecurity, it's worth adding a caveat. Given their role as cybersecurity providers and advisors to their clients, most MSPs do display above-average levels of cyber confidence, especially when compared to other businesses.

It's also worth noting that the number of MSPs who described their cyber confidence levels as average or above (96%) has remained consistent with 2024. 97% of those we surveyed last year rated their cyber confidence levels as 'fair' or 'great'.

What's more, outside the 20% who categorised their cyber confidence as complete, most MSPs (80%) recognised there was some room for improvement. And, as we'll see in the next section, most MSPs have a clear idea of what they need to do to improve their cyber confidence.

Getting to Complete Cyber Confidence

We asked MSPs what they felt would help their business to achieve "Complete Cyber Confidence", a framework we define as:

> "An organisation's trust in its ability to protect its digital assets, data, and systems from unauthorised access, cyber-attacks, and data breaches. This approach goes beyond mere compliance with regulations and encourages a proactive and comprehensive approach to security."

The results were as follows:

9. Which, if any, of the following would help your business to achieve complete cyber confidence? [select all that apply]

1st	Continuous monitoring – of systems and networks to detect unusual activity	52%
2nd	Cyber security training for employees – ensuring staff are aware of security best practices and potential threats	51%
3rd	Proactive risk management – identify and mitigate risks before cybercriminals can exploit them	48%
4th	Cyber secure culture – where employees are aware of threats and proactively report suspicious activity to the business	47%
5th	IT policies – establish and enforce cybersafe conduct	44%
6th	Risk reporting - quantify and assess risks	42%
7th	Incident response plans - having a well-defined response plan in case a security incident occurs	37%
8th	Cyber credentials - external verification and certification of your cyber credentials	37%
9th	None of the above	1%
10th	N/A - nothing in particular / I don't know	0%
11th	Prefer not to say	0%

Response count **722**

These responses give us a crystal clear vision of what MSPs can do to protect themselves and their customers more completely. Three areas for improvement immediately stand out.

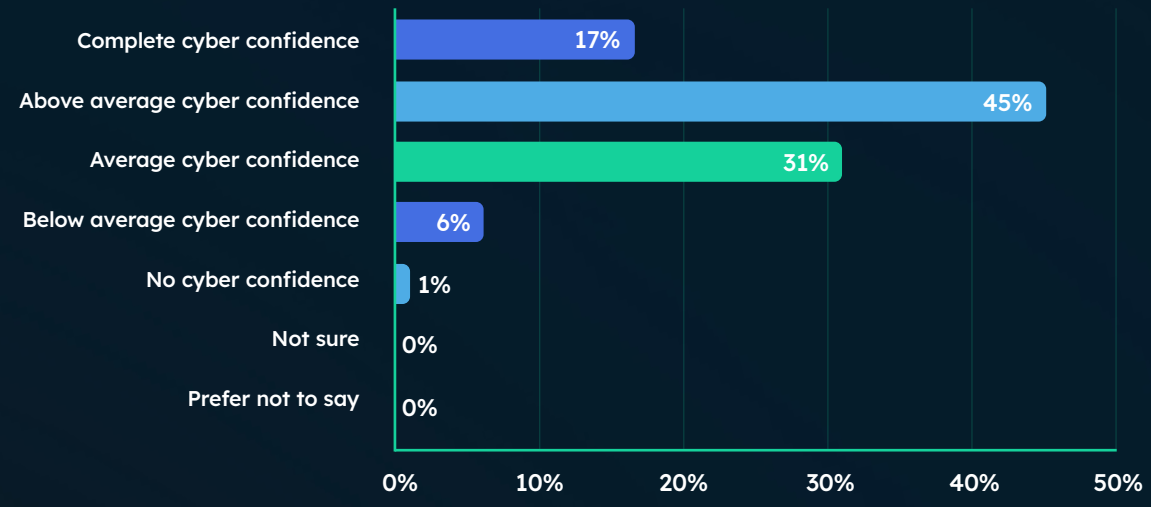
Firstly, there's a clear appetite among MSPs for solutions that allow them to **continuously monitor and detect cyber threats** (52%). This indicates that MSPs are more aware than ever of the need to go beyond "point in time" assessments like **Cyber Essentials certification** and monitor and counter risk year-round.

Second, MSPs recognise the importance of cybersecurity awareness training for employees (51%). It's estimated that **95% of breaches** stem from some form of human error and employee training is by far the most effective way to counter social engineering attacks that prey on human fallibilities, such as phishing and some forms of AI threats.

Finally, MSPs are also prioritising proactive risk management (48%) as a means of countering threats before they become serious.

MSPs are confident in their customers' cybersecurity

10. At what level would you categorise the cyber confidence of your customers?



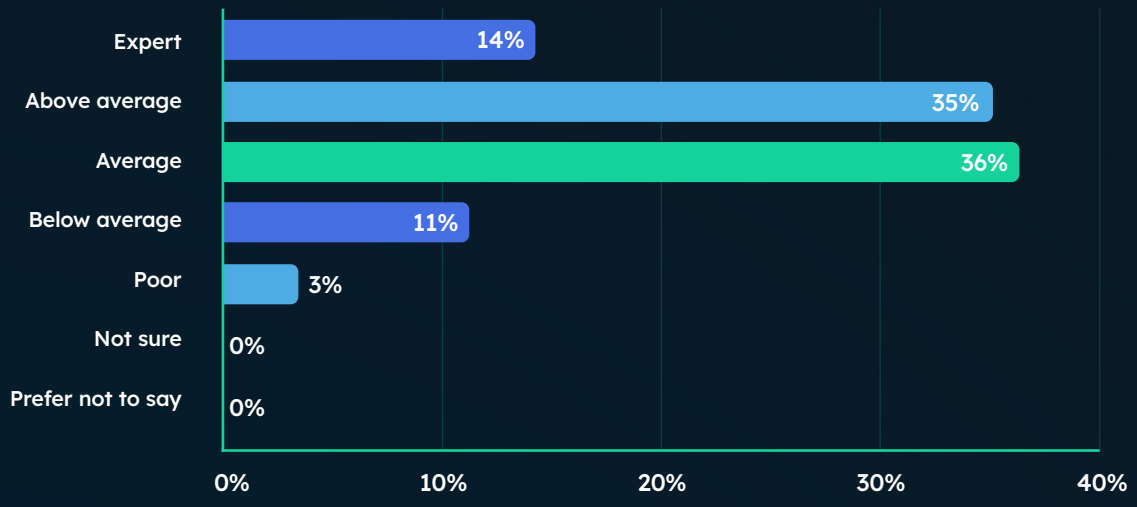
Response count 900

Perhaps counterintuitively, given that **four in ten businesses** suffered a breach in 2024, MSPs' confidence extends to their customers' cybersecurity. The vast majority (93%) of those surveyed rated their customers as having average or above cyber confidence. Many MSPs were more confident still, with 45% categorising their customers as having above average cyber confidence and 17% assessing their clients as possessing complete cyber confidence.

It's a similar story when it comes to customers' cyber knowledge. Most of our respondents (85%) said that their customers had at least average cybersecurity knowledge, with a further 35% assessing customers as above average and 18% as expert.

This is broadly consistent with last year, when 86% of MSPs felt their customers had either a 'great deal' or a 'fair amount' of cyber confidence, and 73% rated clients' cyber literacy as good.

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



Response count **900**

So what's going on? We know from reporting by both the **European Union Agency for Cybersecurity (ENISA)** and DSIT that while societal cyber awareness is improving year-on-year, there's still a lot of room for improvement. What makes MSPs' customers different? Is it overconfidence and cognitive bias on MSPs' part or are their customers simply better prepared?

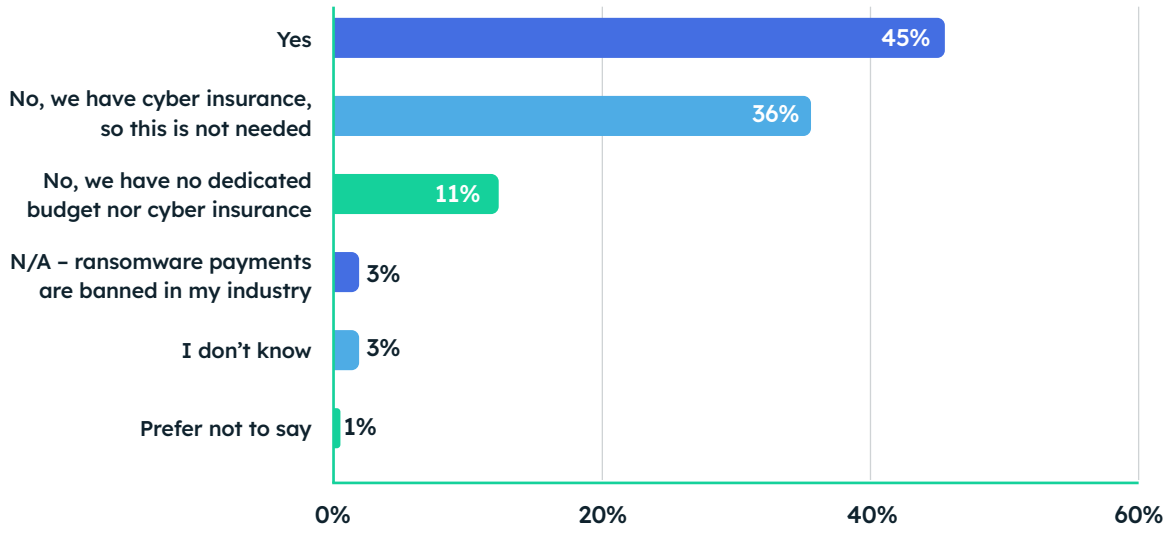
In truth, it's probably a little of both. On the one hand, we've seen evidence that MSPs rate the cyber confidence of both themselves and their customers highly, despite suffering multiple breaches in the last 12 months.

However, on the other hand, MSPs as a sector have done more than any other to drive forward societal improvements in cyber literacy and awareness over the past few years. After all, it's MSPs who advise many businesses on the cybersecurity measures to implement, tools to use, and accreditations to complete. With that in mind, perhaps MSPs are justified in being confident that their clients are far better equipped to deal with cyber threats than the average business.

Confusion reigns over ransomware payments

By far the most surprising result of our survey concerns ransomware payments. Attitudes towards ransomware payments have shifted in the last few years. Many governments, most notably the UK, have mooted bans on ransomware payments for public bodies and government contractors. Meanwhile, cyber insurance providers are increasingly advising clients not to pay ransoms

12. Does the business you work for have a dedicated allocation of money in case of ransomeware attacks?



Response count 900

With that in mind, it was unexpected to see so many MSPs (45%) answer that they kept a dedicated allocation of money in case of ransomware attacks. More worrying still is the 11% of MSPs that have no dedicated budget for ransomware payments or cyber insurance.

What's at the root of this? Well, what businesses should or shouldn't do when it comes to ransomware payments has always been poorly defined. What your business is advised to do will largely depend on where you're based and who's advising you. And this is reflected in our survey results.

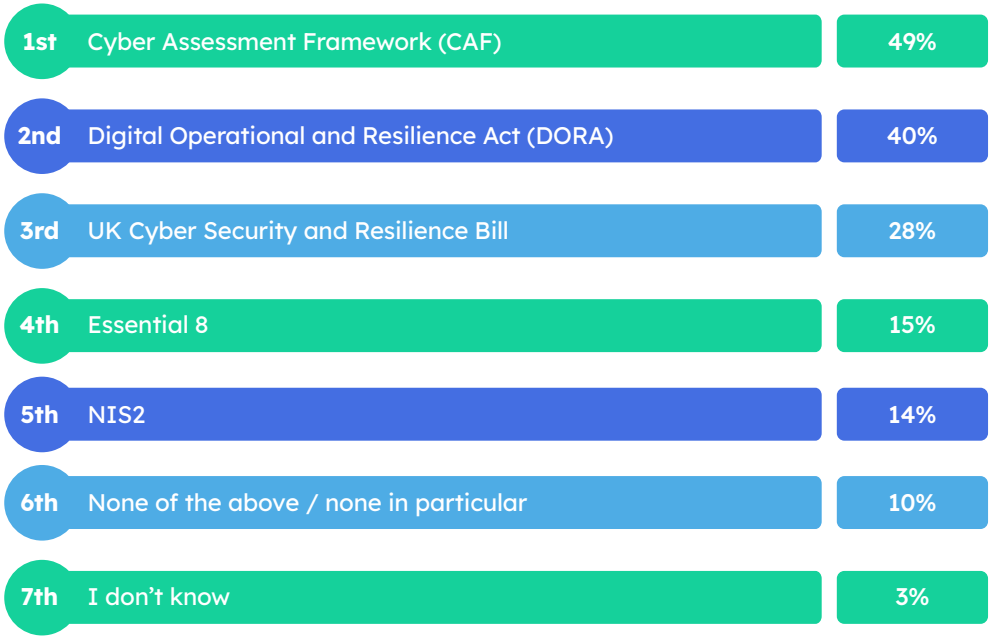
The results appear to indicate that, like everyone else, MSPs suffer from a lack of clarity around best practices for ransomware. What's more, this uncertainty is likely to filter down to their clients, meaning the case for legislative guidance on this issue has never been clearer.

MSPs are concerned but prepared for regulations

For our last questions, we asked MSPs which upcoming regulations and/or legislation they were most concerned about.

As you'd expect, the results were largely predicated on geography, with UK MSPs most concerned about the upcoming Cyber Security and Resilience Bill (28%) and the **Cyber Assessment Framework** (49%). Whereas, MSPs based in the European Union were more concerned with the **Digital Operational and Resilience Act** (40%) and NIS2 (14%). And, naturally, Australian MSPs were focused on Essential 8 (15%).

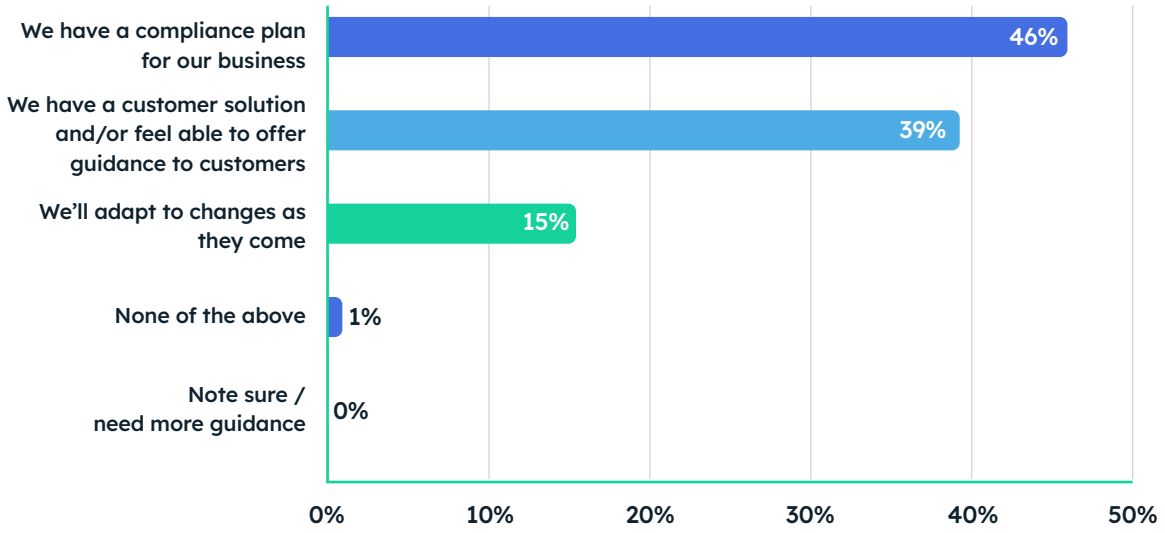
13. With cybersecurity regulations tightening across regions, which regulations or frameworks are you most concerned about/are most relevant to your business? [select up to two]



Response count **900**

However, what's far more interesting is how prepared MSPs are to meet legislative and regulatory changes. Regardless of jurisdiction, a large portion of our respondents were well prepared to meet regulations. 46% said they had a compliance plan for their business, and a further 15% indicated that they were ready to adapt to regulatory changes as and when they happen.

14. Which, if any, of the following describes how prepared you are for compliance with local and international cybersecurity regulations and customer demand for cybersecurity guidance? [select best match]



Response count 900

Another 39% of MSPS felt they were ready to offer a solution or guidance to customers in meeting cybersecurity regulations. This is a healthy figure, however, it's a little unexpected that it isn't higher. Although, in some cases, particularly with NIS2, this may be due to slow progress by states in implementing required laws. It's also worth pointing out that some jurisdictions are further along than others. For example, the figure was far higher for UK MSPs at 57%.

Nevertheless, it's a surprise.

As cybersecurity legislation evolves and compliance obligations become more onerous, MSPs are ideally placed to help businesses get on top of regulation. This is set to be one of the key opportunities for MSPs across 2025 and beyond, so those MSPs not meeting demand could be leaving revenue on the table.

Key takeaways

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

1. MSPs remain a key target for cybercriminals, with 69% experiencing two or more breaches in the last 12 months.

2. Despite high levels of cyber confidence among MSPs, they're still being breached at an alarming rate, suggesting room for improvement in cyber posture.

3. MSPs named continuous monitoring (51%), employee cybersecurity training (51%), and proactive risk management (48%) as the measures most likely to help them improve cyber confidence.

4. MSPs feel their customers are slightly less at risk from cyber threats than in 2024, however, concern levels still remain high.

5. Emerging AI threats pose the number one risk to both MSPs and their clients, closely followed by ransomware and malware.

6. However, MSPs potentially underestimate supply chain attacks as a threat, with just 15% listing it as a major concern.

7. MSPs are confident about customers' cybersecurity levels and overall cyber awareness.

8. 84% of MSPs now manage either their clients' cybersecurity infrastructure or their clients' cybersecurity and IT estate combined. This suggests that last year's trend of MSPs pivoting towards cybersecurity has become widespread.

9. MSPs have invested heavily in meeting customer demand for cybersecurity services:
   - 81% increased spend on specialist cybersecurity hires
   - 78% had upped spending on their security capabilities
   - 60% had invested in specialist regulatory hires
   - 64% had increased spending on regulatory capabilities

10. 45% of MSPs have a dedicated pool of money set aside for ransomware payments, despite insurers and governments increasingly advising against it. This suggests a need for clarity and legislative guidance.

11. MSPs are concerned but prepared for local and international legislation and regulations. However, for many, there is an untapped opportunity to offer guidance and services to help customers comply.


CyberSmart
cybersmart.co.uk