CyberSmart

The CyberSmart MSP Survey 2024

Introduction

Managed service providers (MSPs) form a key vertebrae in the backbone of the UK economy. According to the Department for Science, Innovation & Technology (DSIT) research, the country's 11,000 plus MSPs were worth **£52.6 billion to the UK economy in 2022** alone.

Despite that impressive figure, MSPs' importance to the UK economy exceeds their financial contribution. MSPs often represent a one-stop shop for many SMEs' IT needs, providing and administering everything from office software packages to network security. This makes them a critical first line of defence against cyber threats for small businesses.

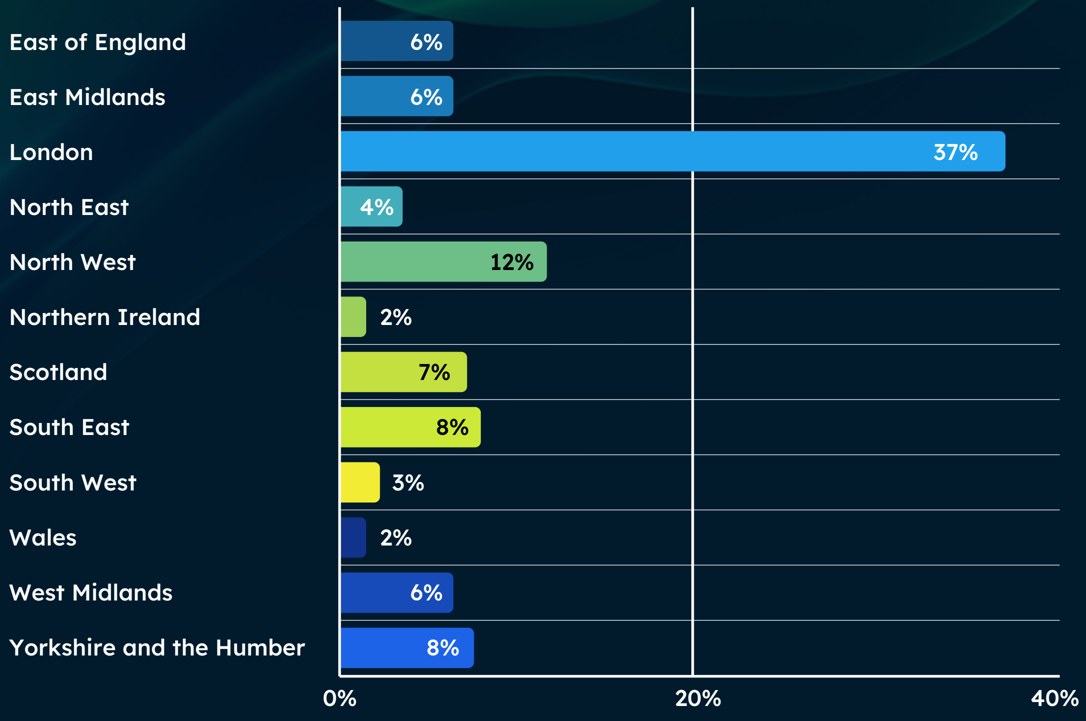
However, the same thing that makes MSPs a cornerstone of our economy has also made them a target. As trusted partners to hundreds of thousands of UK businesses, MSPs typically have access privileges to clients' infrastructure and inner workings – making them a highly lucrative target.

Indeed, a 2024 report from Kaseya reveals that **78% of MSPs view cybersecurity as their greatest challenge**. And, as we'll cover later in this report, they're right to feel that way; almost every MSP we spoke to had experienced a data breach in the last 12 months.

All of this begs the question, given MSPs are such a critical part of the UK's IT infrastructure, why is there so little research (beyond the **UK government's**) into their cybersecurity? How prepared are MSPs and their clients? What are the key threats they face? And, most importantly, how are they managing them?

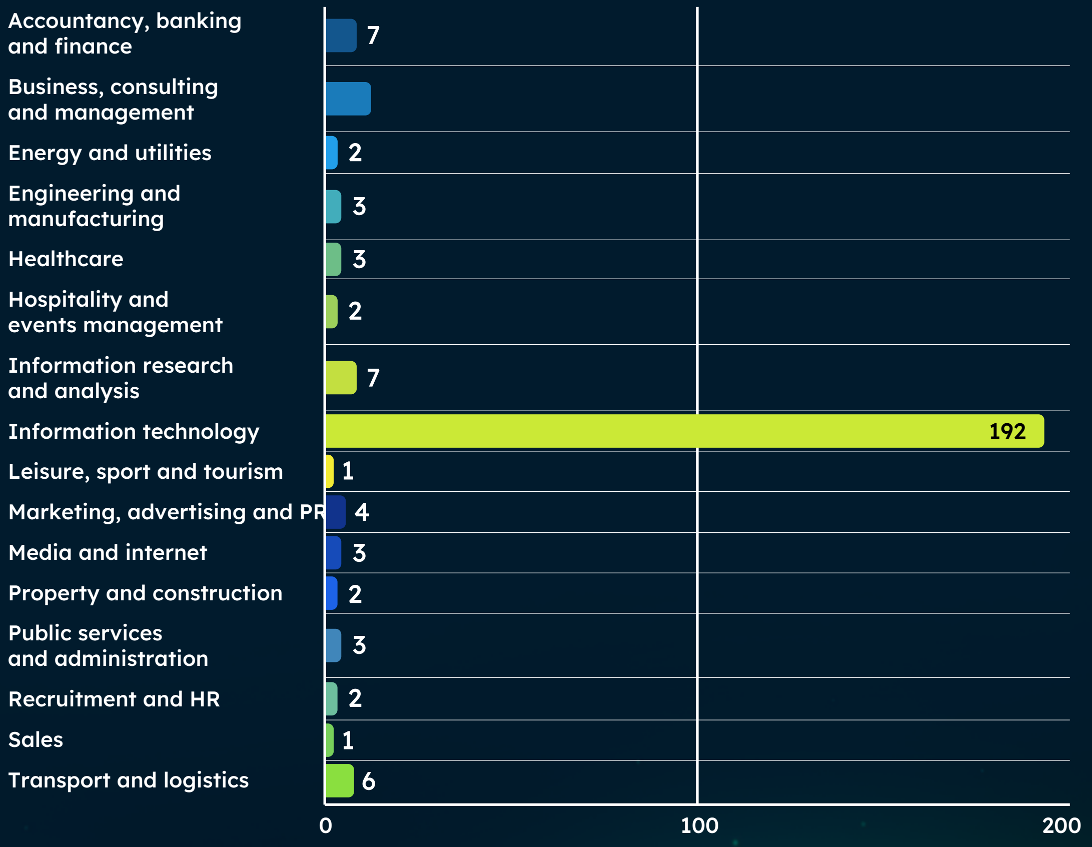
In early 2024, we set out to change this. Alongside **OnePoll**, we surveyed 250 leaders from UK MSPs. To ensure we got a broad spectrum of views, we spoke to MSPs with customers across every major industry, from all over the UK, ranging in size from one to one thousand employees (see table below).

Where do you live?



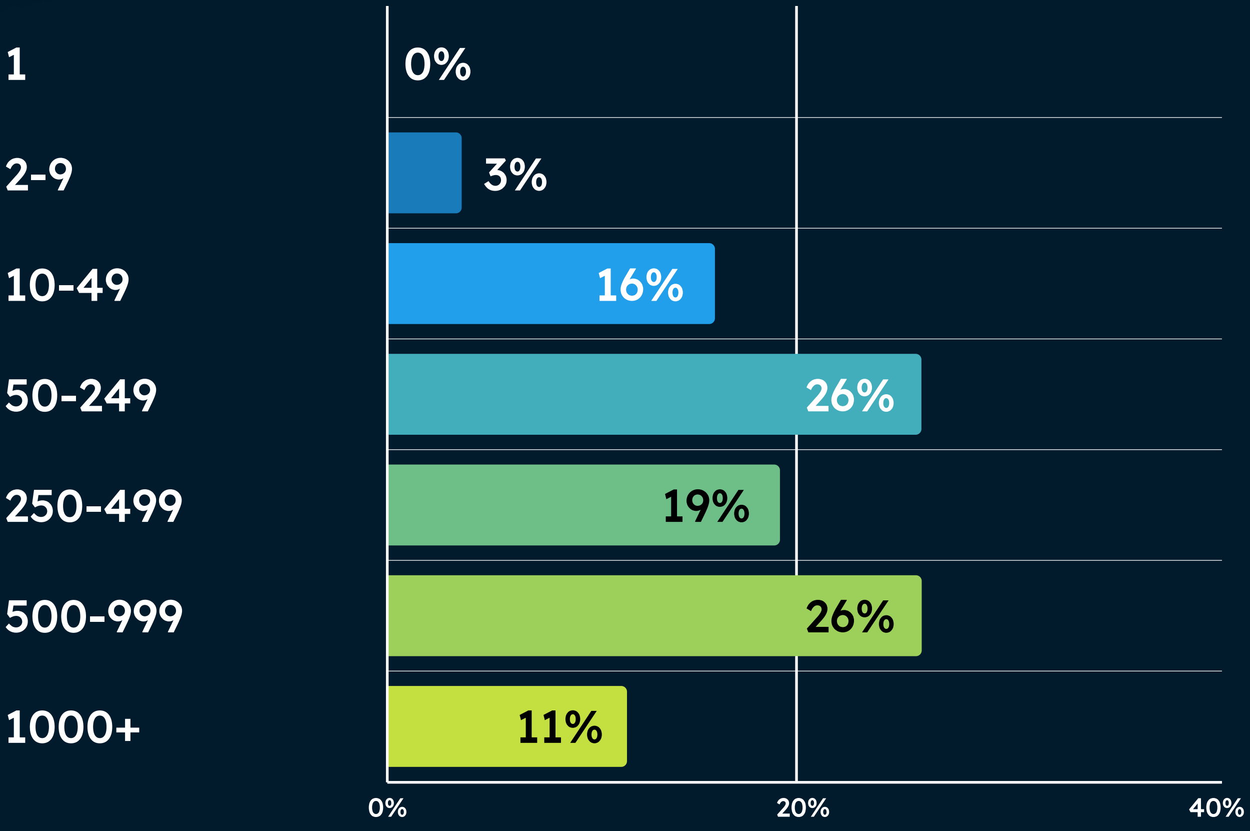
Response count 250

In which industry do you specialise in, with regards to MSP?



Response count 250

How many employees work within the MSP part of your organisation?

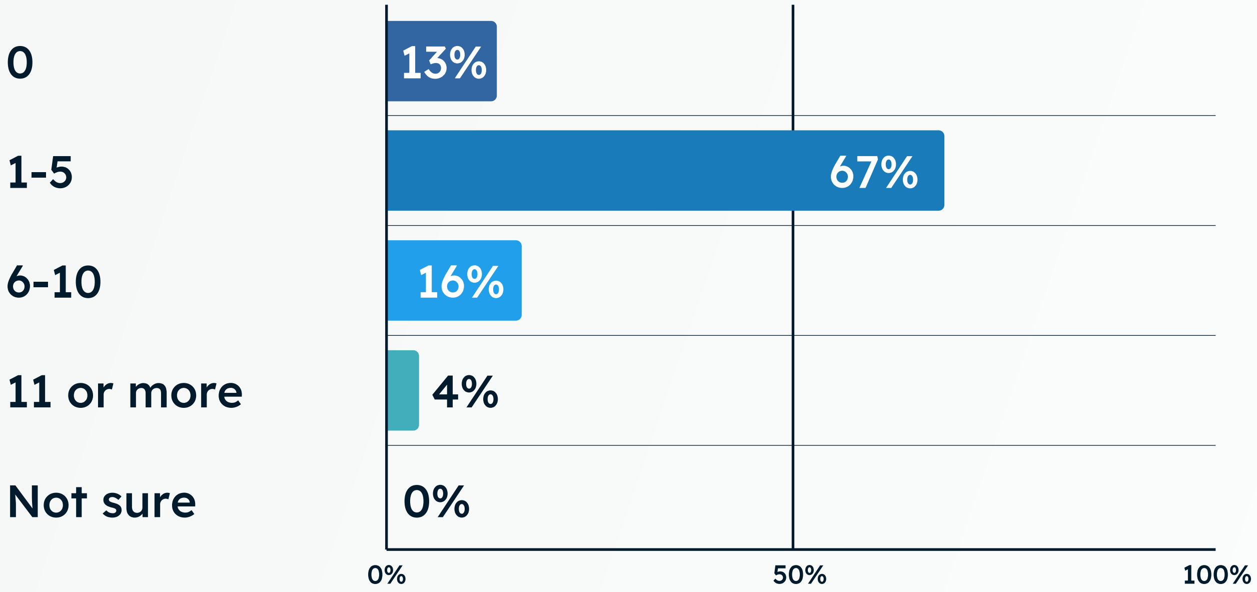


Response count 250

What follows are the results of this study, providing an accurate picture of the cybersecurity landscape for MSPs and their customers in 2024.

MSPs are a key target for cybercriminals

How many cybersecurity breaches have you suffered in the past 12 months, if any? [select best match]



Response count **250**

Let's begin with perhaps the least surprising finding in our report. MSPs continue to be a key target for cybercriminals. However, what might surprise you is how often MSPs are being successfully breached.

A clear majority (87%) of our 250 MSPs reported having experienced at least one data breach in the past 12 months, with many being hit multiple times. This illustrates just how big a threat cybercrime has become to every MSP. What's more, it's not just MSPs with good cyber hygiene. As we'll discuss later, many of these leaders reported having either a 'fair' or 'great' deal of cyber confidence.

Why are MSPs being attacked?

Upon first hearing, it might sound odd that cybercriminals target and often successfully attack MSPs. We think of MSPs as IT and cybersecurity experts with good defences, so surely there are more tempting targets?

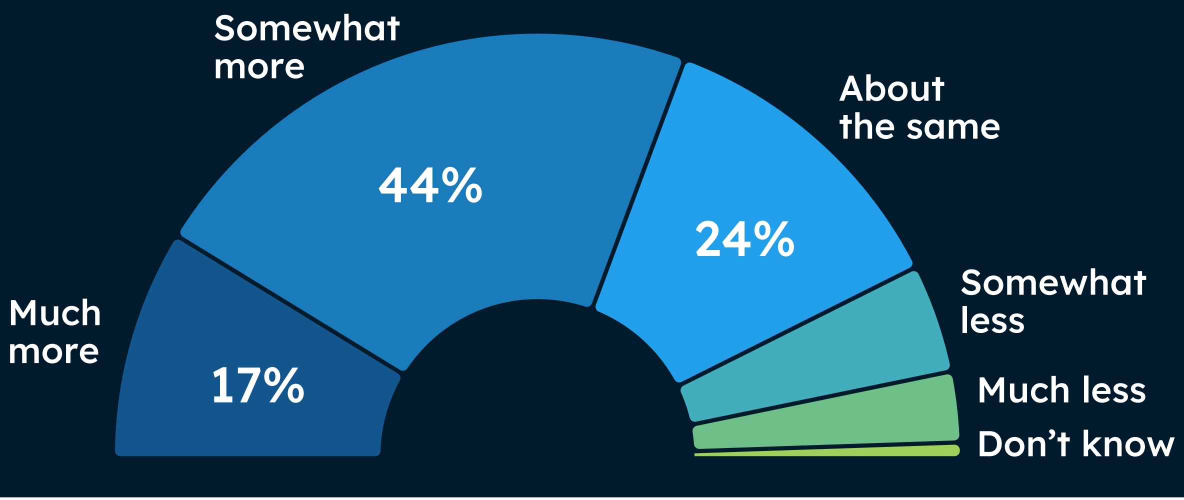
Unfortunately, this is only partially accurate. Although many MSPs do have robust cyber defences, there's another reason they get cybercriminals champing at the bit.

MSPs are so attractive to hackers because they can typically remotely access clients' networks and IT environments. And, that's before we mention how much data the average MSP has access to – everything from financial information to breakdowns of customers' security.

In short, MSPs are targeted for the same reason as **supply chains.** Successfully breaching an MSP means cybercriminals gain access to much more than the initial target. It could lead to 'follow-on' activity across the MSP's customer base.

MSPs feel their customers are more vulnerable to cyber threats

Do you feel your customers are more or less at risk from cyber threats in the last 12 months (2023), compared the 12 months prior (2022)?



Response count **250**

The last year has seen a confluence of factors negatively affecting SMEs' online security, from the **cost of living crisis** to increased **geopolitical tensions** to lowered technical barriers to entry for cybercrime. Given this landscape, it's unsurprising that 60% of MSPs believe their customers have been more vulnerable to cyber threats in the last 6 months.

However, this figure is quite revealing if we dig a little deeper. Cyber awareness is on an upward curve within businesses and society. It's difficult to be unaware of the risks when each news cycle brings a new story on the latest breach. This means the perceived threat of cybercrime is continually increasing as awareness grows.

Indeed, as we'll see later in the report, MSPs are switching to providing cybersecurity services and products in ever-increasing numbers, partly as a response to customer demand. Accordingly, perhaps this fear of customer vulnerability stems from greater awareness of the threats.

What kind of threats do MSPs and their customers face?

We've established that MSPs are hyper-aware of the threat of cybercrime. So, what do they perceive as the biggest threats to themselves and their customers?

MSPs

Which, if any, of the following are the biggest possible threats to your business? [Select up to 3]

1st	Ransomware or malware infection	57%
2nd	Inflation and spiralling costs	43%
3rd	Exploitation of unpatched or undisclosed vulnerabilities	41%
4th	Insider threats	37%
5th	Skills shortages	35%
6th	Supply chain	26%
7th	Slowing sales pipeline	14%
8th	None of the above	0%

In common with their customers, MSPs feel the number one threat is **ransomware** and **malware** (57%). This is followed closely by inflation and spiralling costs (43%), exploitation of unpatched vulnerabilities (41%), and insider threats (37%). Skills shortages (35%) and supply chain security (26%) complete the top six.

This tells us that MSPs have a good grasp of the threats they face. As our **2023 cost of living report** revealed, inflation and its impact on security budgets and staff wellbeing is a major concern for all SMEs, as are insider threats (both negligent and malicious).

However, there are some notable exceptions. Given the large networks many MSPs administer, **supply chain attacks** should be more prominent in their thinking. It's also surprising to see so few MSPs specifically mention phishing scams. DSIT's **Cyber Security Breaches Survey 2024** revealed that the most common type of breach or attack is phishing (84% of businesses and 83% of charities). However, many MSPs possibly viewed phishing as synonymous with ransomware and malware.

What about MSPs' customers?

Which, if any, of the following represent the biggest possible threats to your customers' businesses? [Select up to 3]

1st	Ransomware or malware infection	55%
3rd	Exploitation of unpatched or undisclosed vulnerabilities	44%
2nd	Inflation and spiralling costs	41%
4th	Insider threats	32%
5th	Supply chain threats	31%
6th	Skills shortages	26%
7th	Slowing sales pipeline	12%
8th	None of the above	1%

For the most part, the MSPs we surveyed listed the same biggest threats to their customers as themselves. Ransomware and malware came out on top again (55%) followed closely by exploitation of unpatched vulnerabilities (44%).

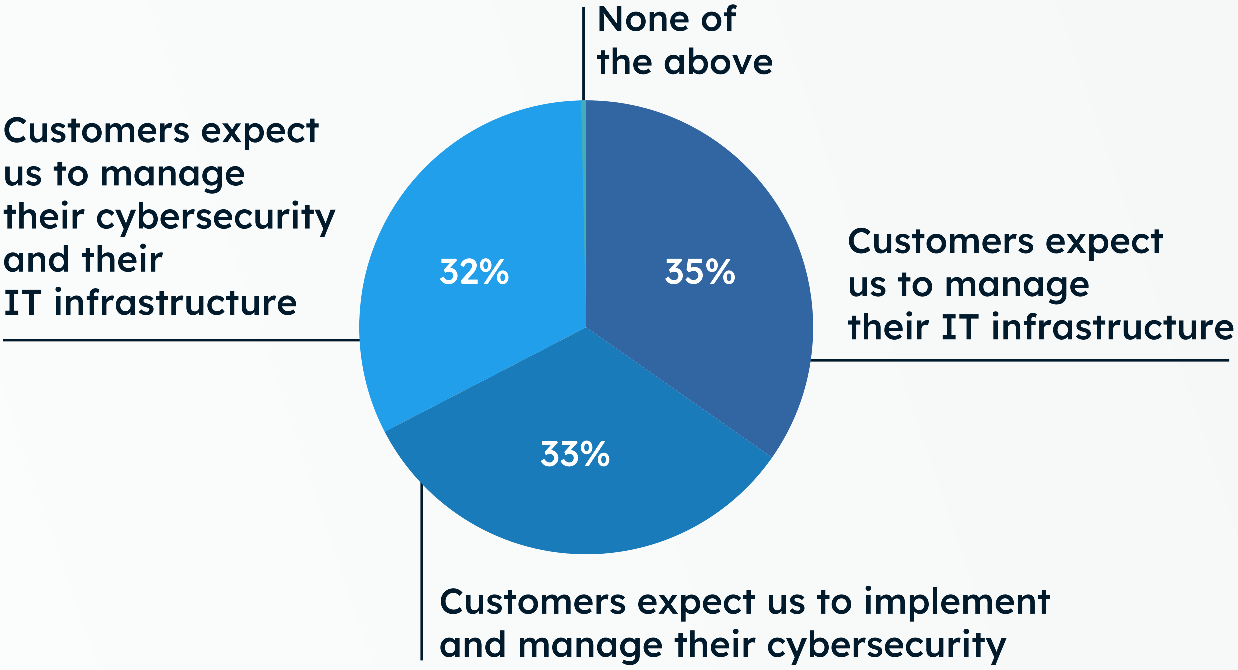
What can we learn from this? Most obviously, MSPs feel they are subject to the same fears as their customers. But it also demonstrates that MSPs are in a great position to understand the security needs of their customers. In many cases, the service provider has implemented many of the same measures they recommend to customers.

The role of the MSP is changing

As signposted by their name, MSPs' traditional role was to provide managed IT infrastructure services to clients. However, our survey points to a shift in what MSPs' customers expect from them and the services they offer.

65% of the MSP leaders we surveyed said that customers now expect them to either manage or implement customers' cybersecurity.

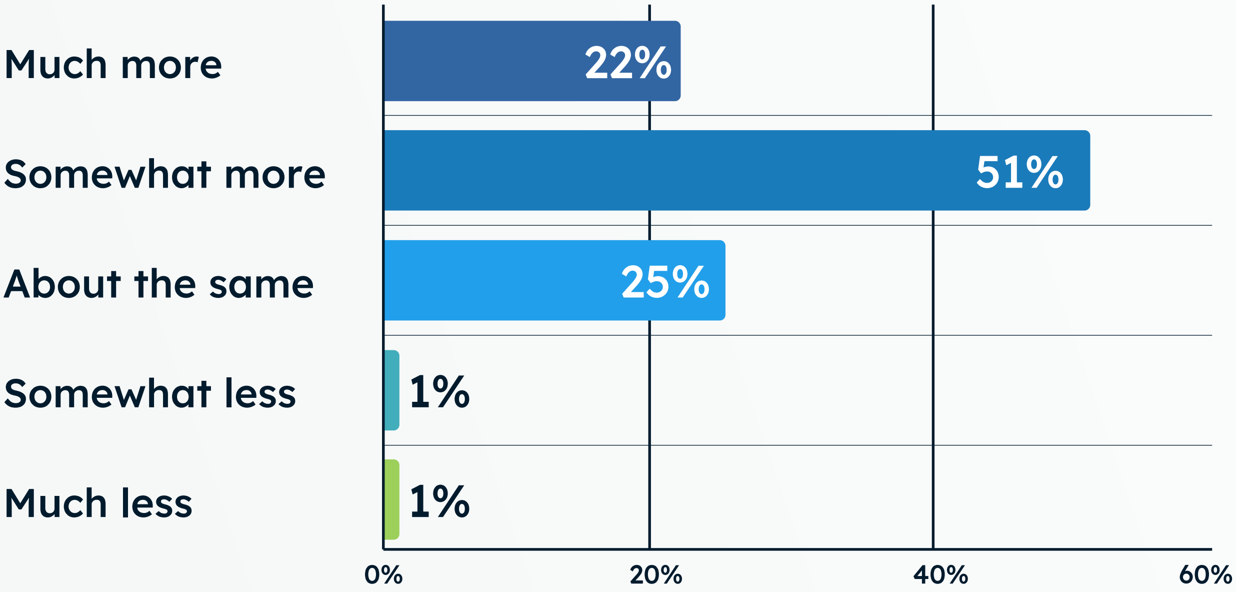
Which of the following best describes your customer's expectations of your services? [select one]



Response count **250**

This has increasingly become a dealbreaker for prospects choosing a managed service provider. Over 70% of MSPs have noticed ‘more scrutiny’ of their security capabilities during new business meetings in the past 12 months.

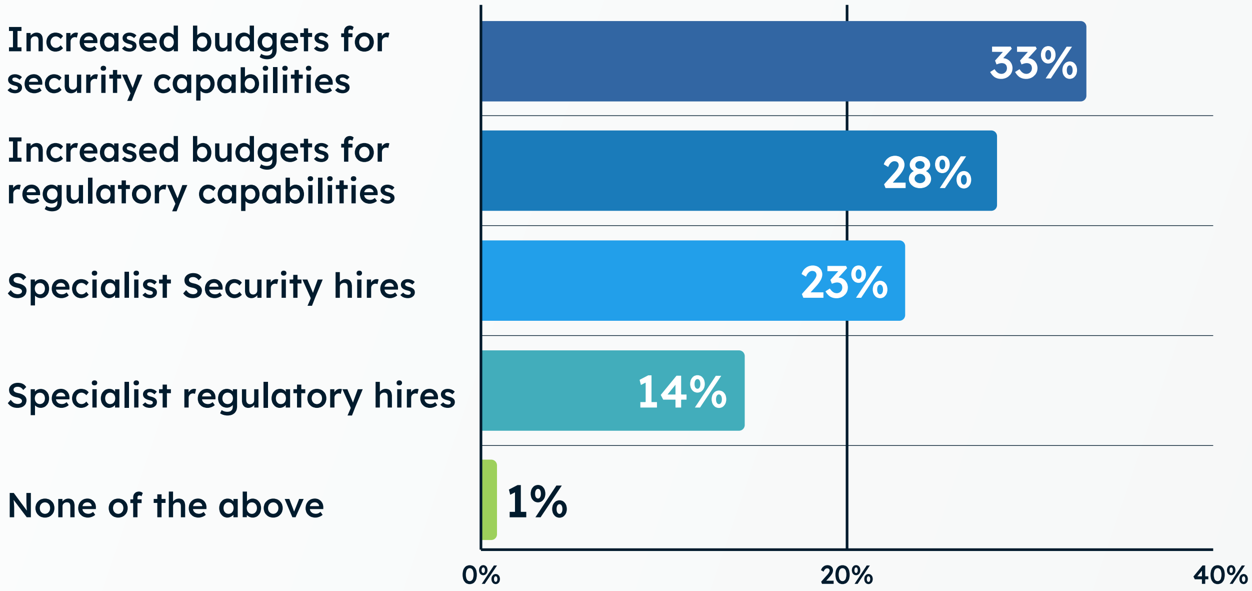
Have you noticed more or less scrutiny placed on your security capabilities during new RFP/ New business meetings in the last 12 months?



Response count **250**

MSPs are responding to the demand

Which, if any, of the following changes have you made in the past 12 months? [select all that apply]



Response count **250**

Managed service providers have long prided themselves on delivering exactly what their customers need to do business. As cybersecurity has become more important to customers, MSPs have rapidly shifted towards offering security and regulation services.

Almost 70% of the companies surveyed have increased their security capabilities over the last 12 months. And, this isn't just an investment in products and services, nearly half have made specialist security or regulatory hires.

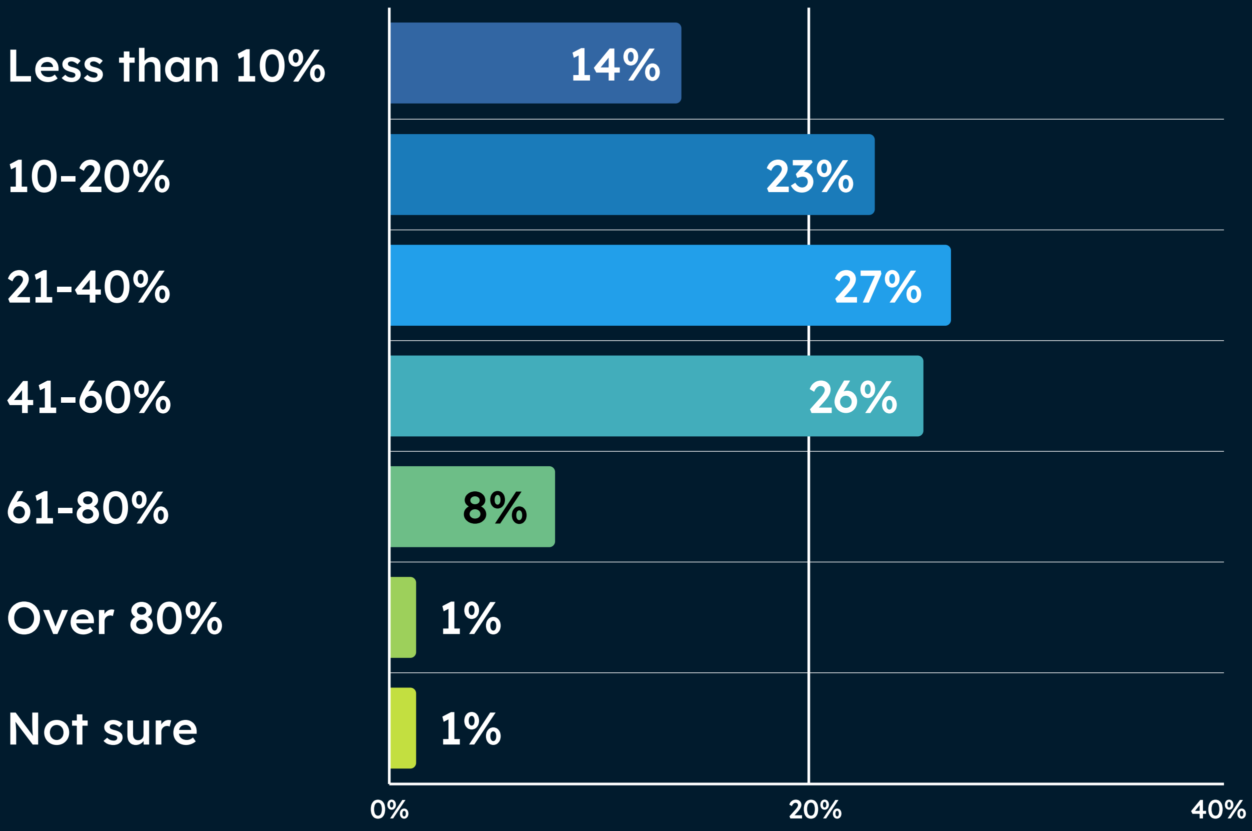
It's clear from their responses that MSPs are leaning into cybersecurity in a big way. This also looks like a permanent trend. **Barracuda estimates** that 83% of UK small and medium enterprises are using some form of IT-managed service and, as these companies look to improve their security, it's only natural that they turn to their MSP for help.

It's a real opportunity for MSPs to become their customers' trusted security provider – more on that in our next section.

A huge opportunity for MSPs

So far we've mostly talked in the abstract about the opportunity changing customer demands presents to MSPs. However, it's also revealed in responses to our survey. 37% of MSPs report one in five or fewer customers have an in-house security team. This means that, for many providers, a substantial chunk of their customer base requires managed cybersecurity services – representing a rich source of revenue for those MSPs ready to grab it.

What percentage of your customers have a specific cybersecurity role at their organisation? [select best match]



Response count 250

This is backed up by DSIT's research into the sector, which reveals that of nearly 11,500 active MSPs, just 3,000 currently offer cybersecurity-related solutions to their customers. This constitutes a golden opportunity for any MSP ready to provide cybersecurity services to get a headstart on the competition and tap into an emerging market.

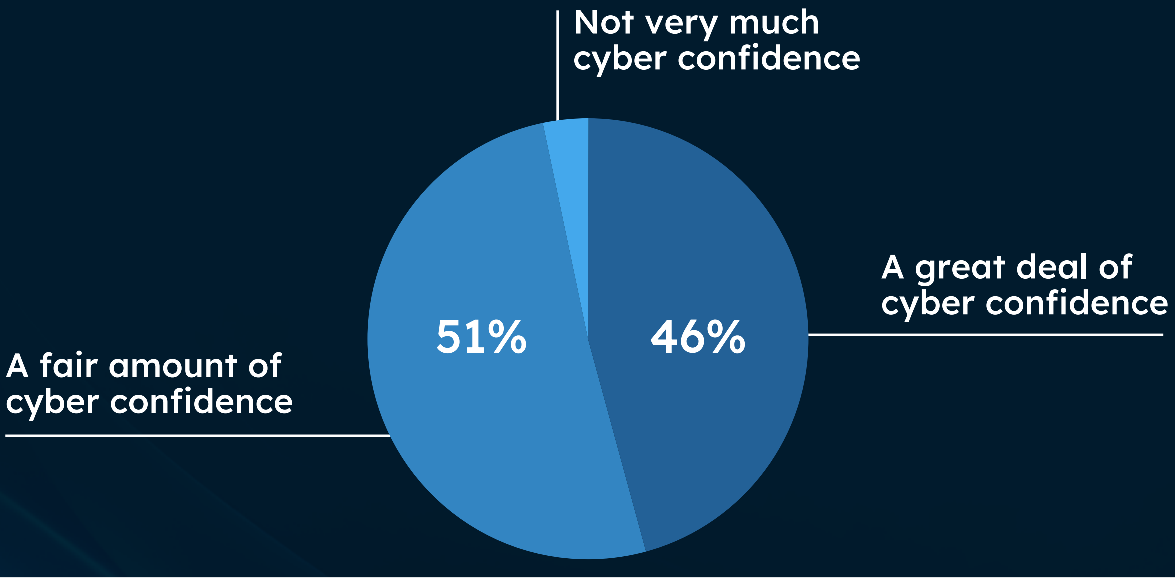
Cyber confidence is high among MSPs and their customers

At the end of the survey, we asked our MSP leaders about cyber literacy and confidence. We defined cyber confidence as engaging in the following activities or processes:

- **Proactive risk management**
- **Continuous threat monitoring**
- **Incident response and/or recovery plans**
- **Cyber training in place for employees**
- **Risk reporting**
- **IT policies in place**
- **Demonstrable cyber credentials**

Nearly all of our respondents ranked their business as possessing a 'fair amount' or 'great deal' of cyber confidence.

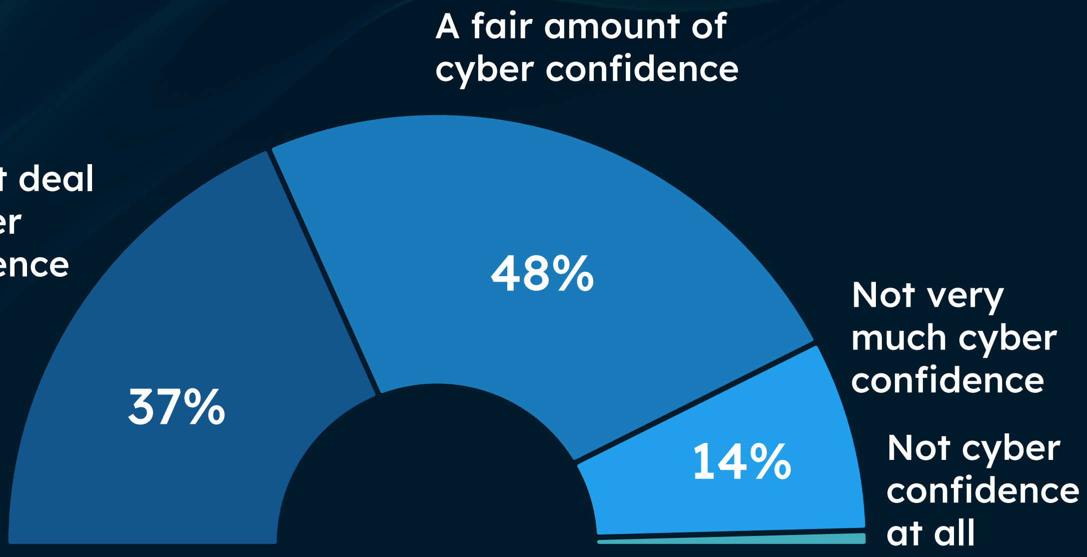
How much 'cyber confidence' does your organisation have?
Engaging in the following activities or processes for example: Proactive risk management, Continuous threat/risk monitoring, Incident response and/or recovery plans, Cyber training in place for employees, Risk reporting, IT policies in place, Demonstrable cyber credentials (e.g. CE or ISO)



Response count **250**

It's a similar story when it comes to MSPs' customers too. 86% of MSPs felt their customers had either a 'great deal' or a 'fair amount' of cyber confidence.

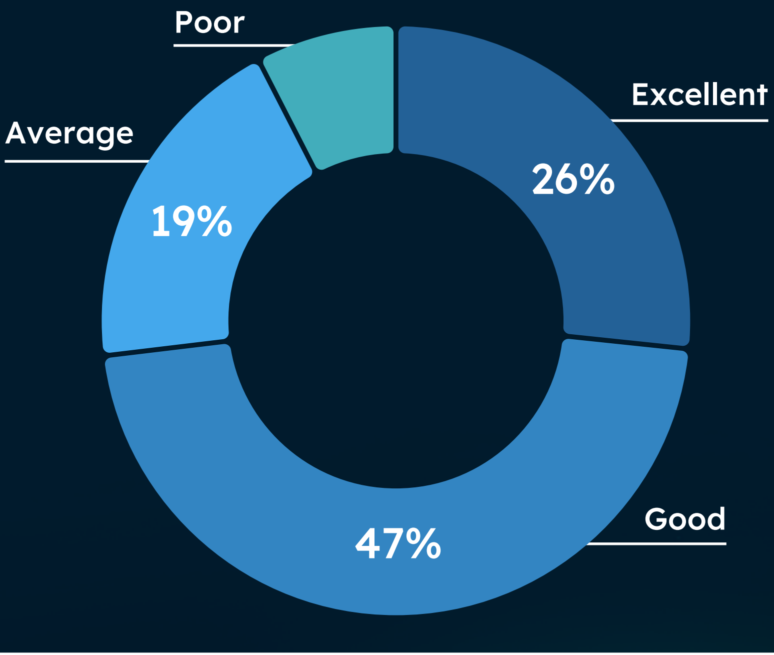
How much cyber confidence would you say your customers have?



Response count 250

MSPs also rated general cyber literacy highly among their customers. 73% said customers displayed either 'excellent' or 'good' cyber literacy, with just 19% and 9% respectively feeling their clients had an average or poor grasp of cybersecurity.

How would you describe the cyber literacy of your typical customer?



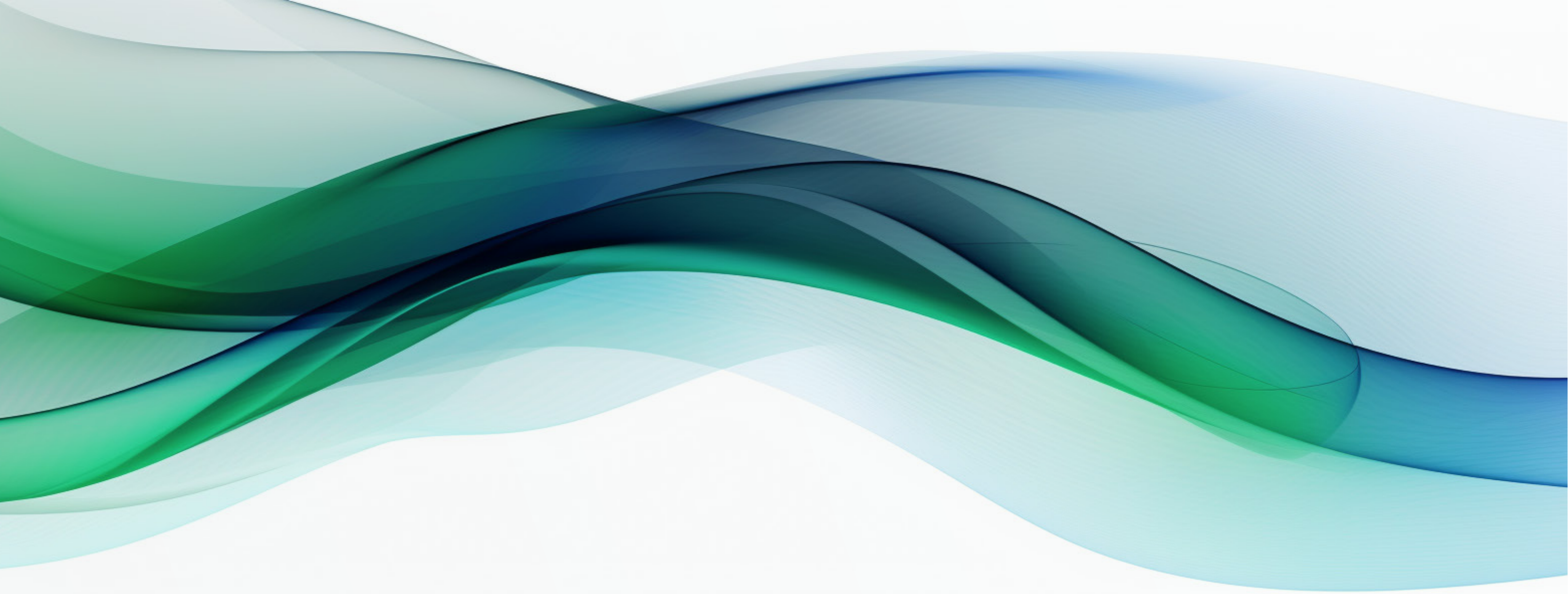
Response count 250

Our findings are borne out by DSIT’s Cyber Security Breaches Survey 2024. Government research discovered that, while awareness of schemes like Cyber Essentials has declined, basic cyber hygiene – by which we mean basic cyber controls – is increasing across all businesses.

Most cyber threats are relatively unsophisticated so organisations can go a long way towards protecting themselves by simply adopting simple measures. And most businesses and charities have a broad range of these measures in place. These include:

- **Using up-to-date malware protection (up from 76% to 83%)**
- **Restricting admin rights (up from 67% to 73%)**
- **Network firewalls (up from 66% to 75%)**
- **Agreed processes for phishing emails (up from 48% to 54%)**

This suggests that MSPs and their customers have become more cyber-savvy and collective security awareness is increasing. Nevertheless, there’s still work to be done, as we’ll see in our next section.



Getting to Complete Cyber Confidence

Although it's a positive development that cyber confidence is so high among MSPs and their customers, that doesn't mean it can't improve further. The eagle-eyed reader will have noticed that despite reporting high levels of cyber confidence, MSPs are still being breached at an alarming rate.

What's going on?

Well, the high breach numbers suggest areas of cybersecurity that MSPs aren't so strong on. This is a normal part of the graduation process from cyber confidence to Complete Cyber Confidence.

Complete Cyber Confidence is CyberSmart's cybersecurity framework, we define it as

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

Using this framework, we asked MSPs which cybersecurity measures should be strengthened to achieve Complete Cyber Confidence.

The measures were:

1st	Cyber security training for employees - ensuring staff are aware of security best practices and potential threats	60%
2nd	IT policies - establish and enforce cyber-safe conduct	57%
3rd	Cyber secure culture - where employees are aware of threats and proactively report suspicious activity to the business	56%
4th	Continuous monitoring - of systems and networks to detect unusual activity	49%
5th	Proactive risk management - identify and mitigate risks before cybercriminals can exploit them	49%
6th	Incident response plans - having a well-defined response plan in case a security incident occurs	40%
7th	Cyber credentials - external verification and certification of your cyber credentials	39%
8th	Risk reporting - quantify and assess risks	36%

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

First, it's clear from the responses that MSPs feel that more needs to be done to give staff the knowledge they need to counter cyber threats. This reduces the risk of negligent insider threats and gives businesses an extra line of defence against anything that makes it past technical controls. MSPs can do this by offering cyber awareness training internally and to customers.

Second, MSPs need the ability to monitor and proactively manage risk across their network and clients' IT infrastructure. In short, they require a way to identify and resolve vulnerabilities before cybercriminals can exploit them.

Key takeaways

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

1. MSPs and their customers remain a key target for cybercriminals with some 87% experiencing at least one breach in the last 12 months.

2. Ransomware and malware are the biggest concerns for MSPs and their customers.

3. Customers increasingly expect MSPs to provide cybersecurity services alongside IT infrastructure – so much so that it's become a dealbreaker. This represents a huge revenue growth opportunity for those providers ready to take it.

4. Despite the high number of attacks on MSPs, our respondents proved remarkably confident in their cybersecurity and that of their customers. However, there was an acknowledgement among all MSPs that there were further steps they could take to achieve Complete Cyber Confidence.

5. Our survey identified some key measures that would help MSPs achieve Complete Cyber Confidence, such as staff training, company security policies, continuous monitoring and proactive risk management. This gives MSPs and vendors like CyberSmart a clear framework to work from.

About CyberSmart

CyberSmart is an all-in-one cybersecurity monitoring, optimisation, training and insurance platform proven to defend against the unexpected.

Why partner with CyberSmart?

CyberSmart is the UK's leading cybersecurity solution for Managed IT Providers.

Join our Partner Programme and get all the software, expert support, and resources you'll need to be the partner your clients can't live without. Expand your portfolio, extend your reach through new solutions and win more business effortlessly, with CyberSmart.

Head to

https://cybersmart.co.uk/partners/partner-with-cybersmart/

to find out more.

CyberSmart