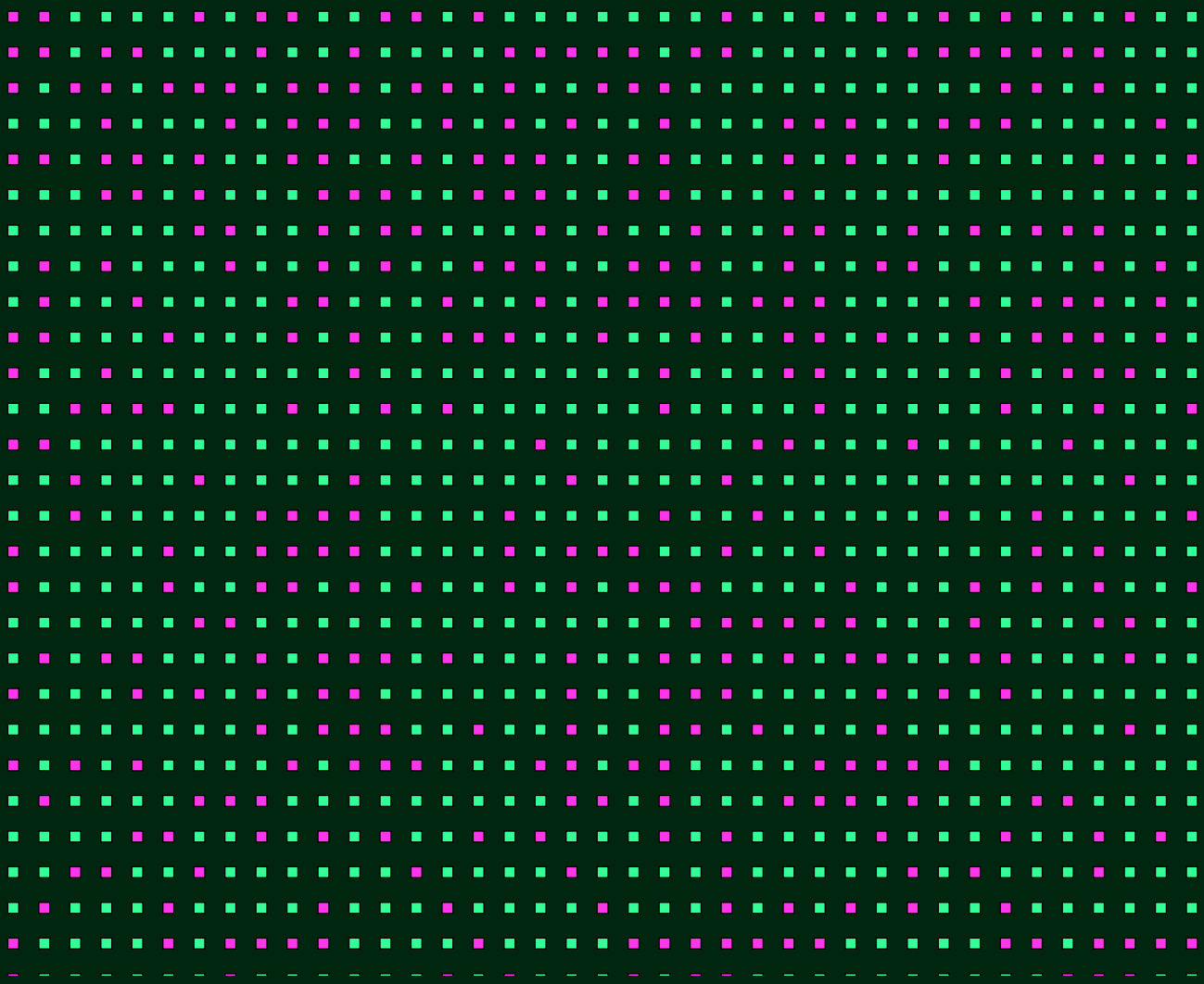
IT & MSP Edition

The state of information security report 2025



Public V1.0

Introduction

Senior security leaders in IT and managed services are operating at the sharpest edge of the cyber risk spectrum.

They're defending highly connected, always-on environments that often underpin other organisations' operations as well as their own. Outages, breaches or service disruptions don't just hurt them; they have the potential to cascade through customer and partner ecosystems.

Our latest State of Information Security Report paints a picture of a sector that is both under intense pressure and quietly confident. IT and managed service organisations are wrestling with AI-driven threats, escalating regulatory expectations and an increasingly fragile supply chain. At the same time, they are investing heavily in new controls, governance and resilience, and seeing tangible business returns from doing so.

This report explores what the data tells us about where the sector is today, where it is heading, and the kind of structured, joined-up approach that will be needed to keep pace.

A sector acutely aware of its own risks

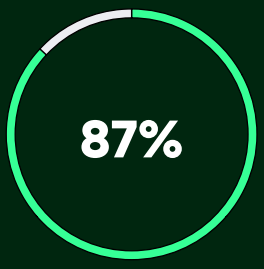
None of our respondents in IT and MSP organisations underestimates the difficulty of their security remit.

Nearly two-thirds (63%) say that the nature of their industry makes it particularly challenging to implement effective information security measures. That's hardly surprising for businesses that:

- Operate complex, multi-tenant and multi-cloud environments
- Are deeply embedded in distributed customer networks and processes
- Provide critical connectivity and services that others depend on, with relentless uptime expectations

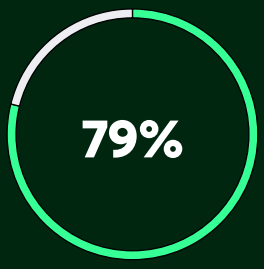
The supply chain only heightens that exposure. Almost two-thirds (63%) agree that security risks originating from third parties and partners are now "innumerable and unmanageable". And these aren't abstract concerns: 66% have been impacted by a security incident caused by a third-party vendor or supply chain partner in the last 12 months, often resulting in data theft (39%), financial loss (36%) and operational disruption (35%).

Yet there is a remarkable sense of optimism within the sector:



say their organisation has a clear and well-communicated information security strategy or policy in place

are confident in their ability to respond to a major cyber incident



say their overall confidence in cybersecurity has increased in the last year

In other words, leaders recognise the scale of the challenge, but they also feel they have a plan.

An attack surface defined by scale, speed and service demands

The data shows just how broad and dynamic the attack surface has become for IT and MSP providers. Leaders are dealing with a dense cluster of challenges that overlap and reinforce one another.

Core operational challenges

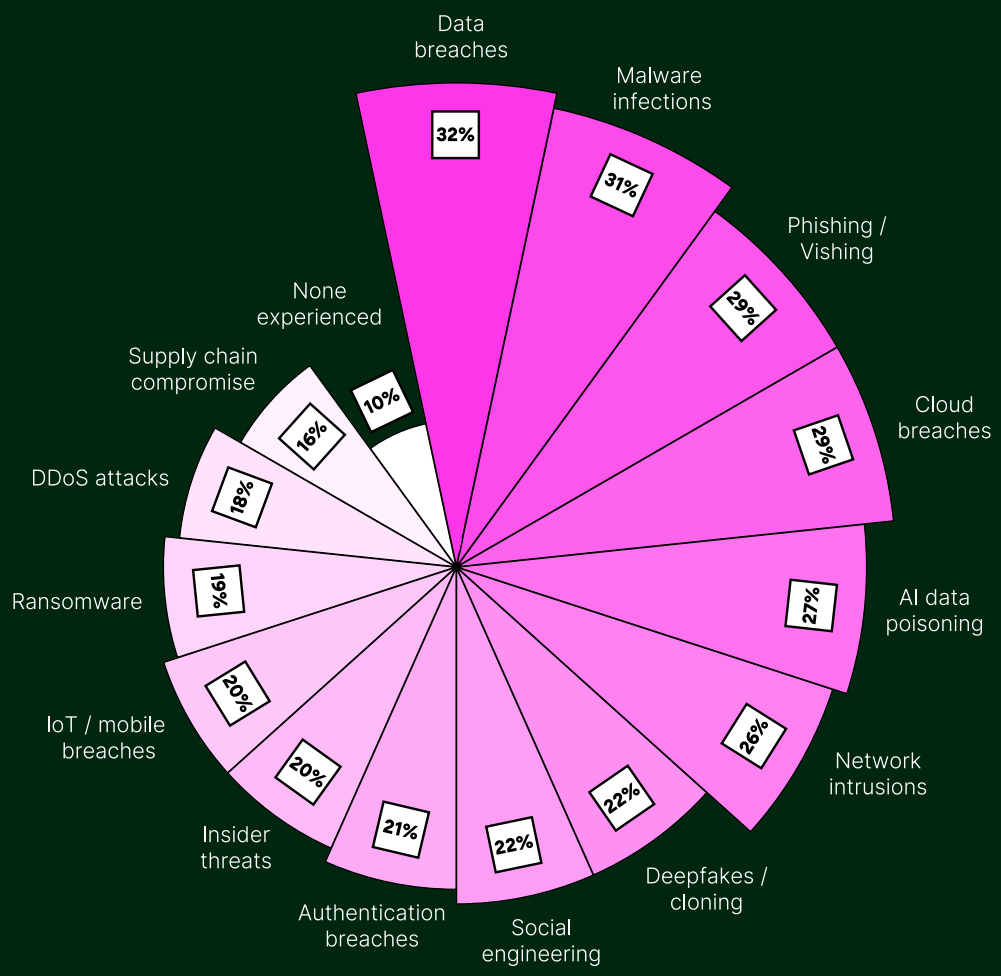
What, if anything, are the challenges you are currently facing in information security?

Taken together, these numbers tell a familiar story: rapidly expanding digital infrastructure, layered with complex obligations, managed by teams stretched thin.

Tech sprawl is particularly significant in this sector, where providers have accumulated multiple point solutions across customer environments, internal platforms and legacy systems. A third (33%) also see securing cloud services as a significant challenge, and 28% cite IoT and BYOD devices, reflecting how deeply mobility, remote access and embedded software now run through service delivery.

Real incidents, not hypothetical risks

These challenges are translating into concrete security events. Over the past 12 months, IT and MSP organisations reported:



What types of cybersecurity/ information security incidents has your business experienced in the last 12 months, if any?

Only 10% say they escaped the year without any kind of incident.

The impact is not limited to IT logs and dashboards. In the last 12 months:

- Customer and employee data were each compromised in 36% of organisations
- Research data (34%), financial data (33%) and product data (31%) were also frequently affected
- Almost a quarter (25%) experienced compromise of personally identifiable information, and 27% saw IP impacted

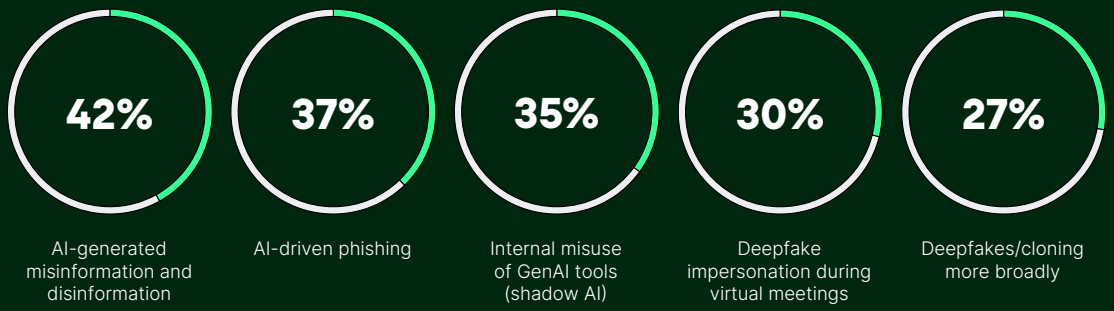
These compromises commonly lead to internal investigations, direct financial loss, system downtime, breach notifications and, in many cases, regulatory scrutiny and fines.

AI: The sector's biggest accelerator, and its sharpest risk

If there is one theme that dominates this year's findings, it's AI.

Leaders are worried, and with reason

When asked about their biggest emerging threat concerns for the next 12 months, IT and MSP leaders put AI risks at the top:



What, if anything, are your biggest emerging threat concerns for the next 12 months?

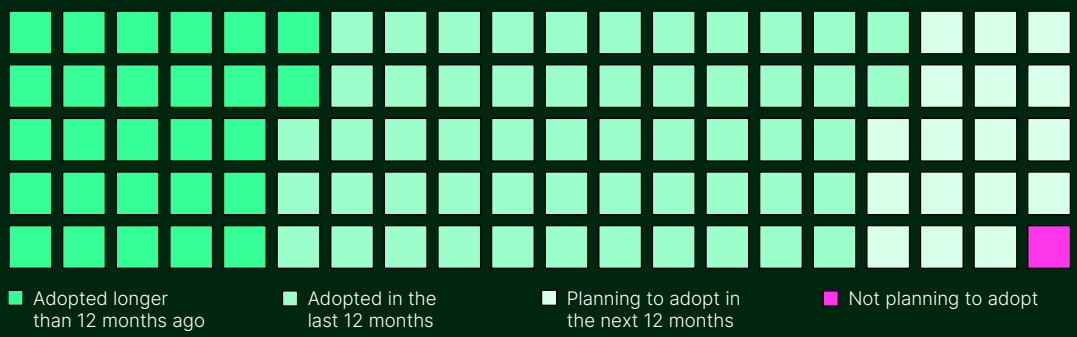
Traditional threats such as ransomware (20%) and supply chain compromise (24%) still feature, but it's clear the centre of gravity has shifted towards AI-enabled attacks and misuse.

This concern is grounded in lived experience. Over a quarter (27%) have already experienced AI data poisoning incidents. And 54% agree that AI and ML technologies are currently hindering their organisation's information security capabilities, even as they promise long-term benefits.

Adoption raced ahead of control

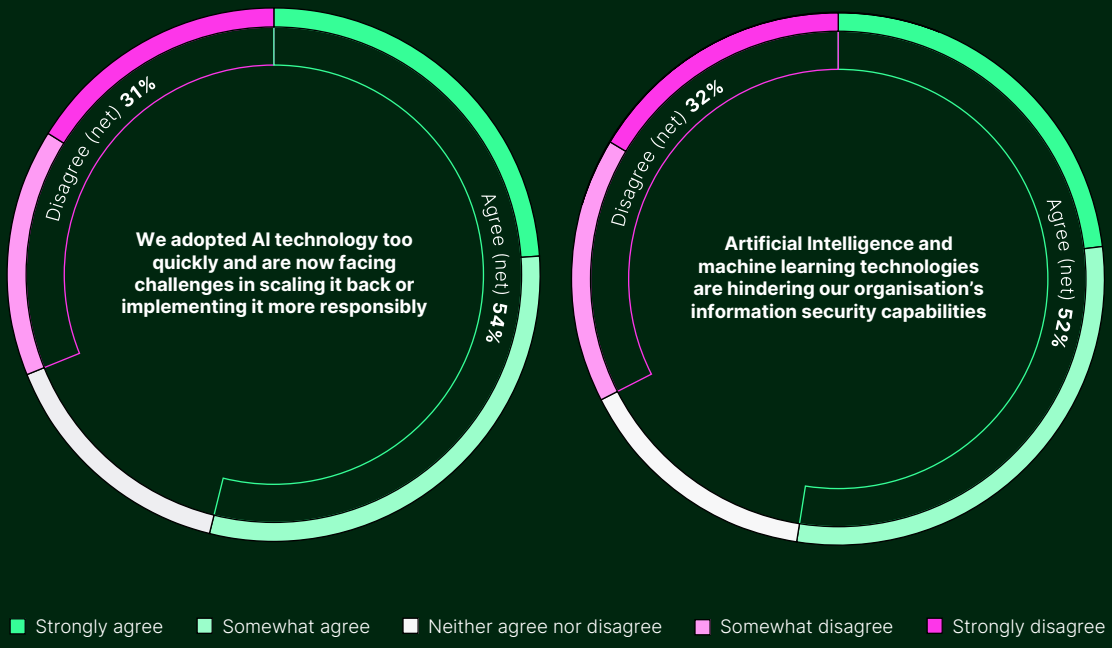
This sector has embraced AI faster than most:

- 81% have adopted new technologies such as AI, machine learning or blockchain
- Most did so recently: 55% adopted in the last 12 months



In the last 12 months have you adopted new technologies such as artificial intelligence, machine learning or blockchain for security, or are you planning to adopt in the next 12 months?

Many now feel the pace was too fast. Over half (56%) agree they adopted AI technology too quickly and are now struggling to scale it back or implement it more responsibly. AI is also reshaping teams: 68% say advances in AI are blurring the responsibilities and scope of traditional security roles.



To what extent do you agree or disagree with the following statements about the current state of the information security landscape?

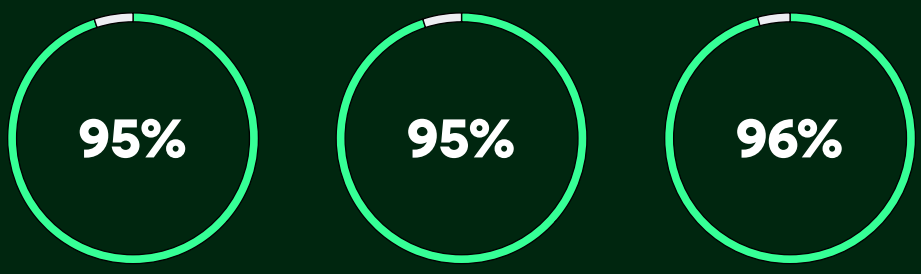
Meanwhile, employee behaviour is compounding the challenge:

- Shadow IT (downloading unapproved software, extensions or services) – 44%
- Using GenAI tools without organisational permission or guidance – 38%
- Using personal devices for work purposes without proper security measures – 35%

In practice, this means sensitive data flowing into unsanctioned tools, inconsistent controls across environments, and fragmented visibility over how AI is actually being used.

A decisive pivot towards AI governance and defence

The good news is that leaders are not standing still. They're investing heavily in bringing AI under control and using it on their own terms:



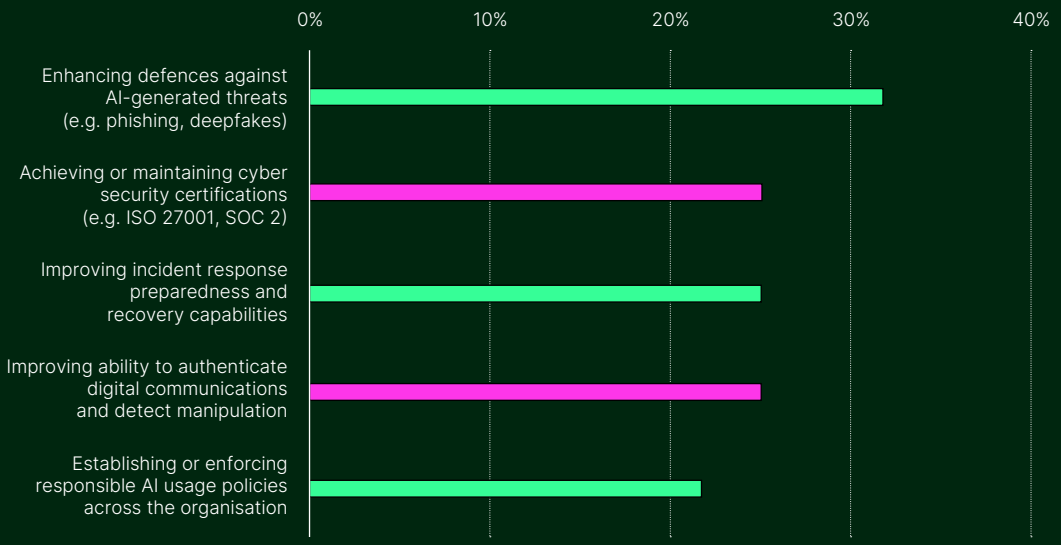
plan to invest in AI governance and policy enforcement in the next 12 months

will invest in deepfake detection and validation tools

will invest in GenAI threat detection and defence

And AI-related priorities are clearly visible in their 12-month roadmap:

- Enhancing defences against AI-generated threats is the number one priority (31%)
- Achieving or maintaining cybersecurity certifications and improving incident response both sit at 25%
- Improving the ability to authenticate digital communications and detect manipulation is also a top-tier priority (25%)
- Establishing or enforcing responsible AI usage policies is a priority for 21%



What, if anything, are your organisations top information security priorities for the next 12 months? (AI-related responses)

Perhaps most strikingly, IT and MSP leaders feel prepared for AI-driven threats. Across categories such as AI-generated phishing, deepfake impersonation, data poisoning, and identity spoofing in virtual meetings, between 86% and 90% say they are at least somewhat prepared.

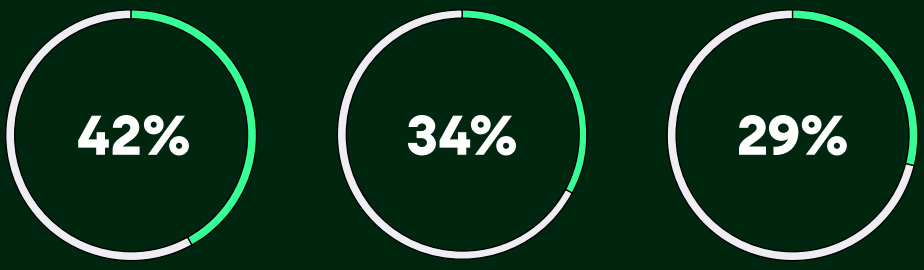
There is a tension here: AI is seen as both a hindrance and an area of high preparedness. The likely explanation is that controls and tooling are maturing quickly, but internal processes, roles and governance are still catching up. This is precisely the kind of environment where integrated, standardised information security management systems become critical.

People & process – the real constraint on resilience

Technology may define the attack surface, but people and process shape the defence. The data this year highlights just how much strain these foundations are under.

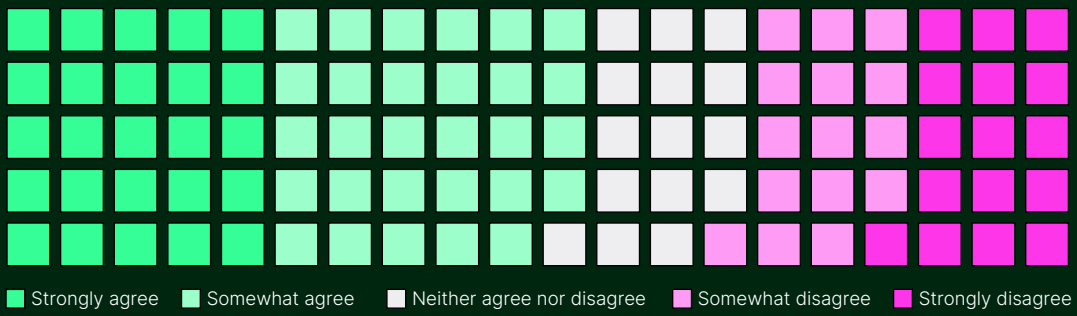
Skills, burnout and leadership remain defining constraints

Core people-related challenges include:



Many organisations have responded by increasing security headcount and outsourcing, but resource pressure remains a constant undercurrent.

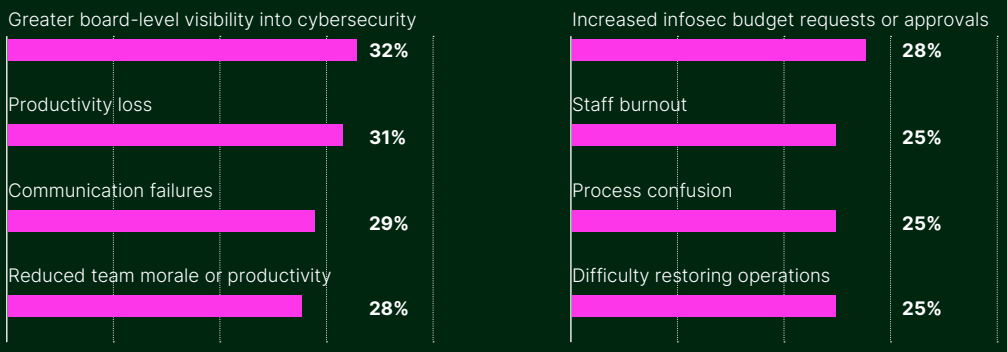
Leadership support is mixed. Half (50%) agree that senior leadership still treats information security compliance as an afterthought, a sentiment difficult to reconcile with the sector's exposure and regulatory load.



To what extent do you agree with the following: Senior leadership at my organisation doesn't understand the importance of information security compliance and treats it as an afterthought

What happens after a breach?

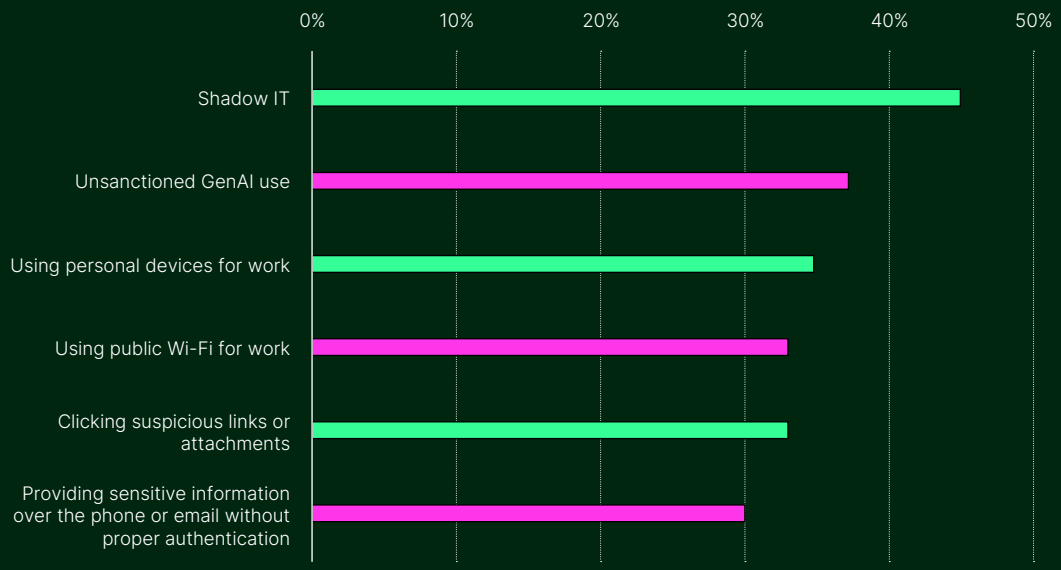
When incidents do occur, the fallout is not only technical.
Among organisations that experienced breaches, common people/process challenges included:



In other words, breaches are forcing governance and process conversations that many organisations have postponed. For some, that's becoming a catalyst for more structured, repeatable ways of managing security and compliance.

The everyday security habits that still slip

Employee actions continue to open gaps, even in mature environments.
Over the last 12 months, common mistakes included:



What, if anything, are the common types of information security/ cybersecurity mistakes made by your employees in the last 12 months?

This reinforces a simple point: security only works when it's both understood and embedded. Organisations need consistent processes, clear policies, and a way to embed those into daily work – especially in distributed, service-oriented businesses where employees and contractors sit across multiple locations and client environments.

Compliance: from cost centre to growth driver

Compliance is often described as a burden, and there are real pressures here. However, the sector's data tells a more nuanced story – one where structured compliance programmes are increasingly seen as an enabler of growth, trust and better decision-making.

Why this sector invests in security and compliance

The top motivations for ensuring strong information security and compliance are both defensive and strategic:

- Boost ability to securely adopt new technologies – 47%
- Protect customers and business information – 45%
- Defend against sophisticated cyber threats – 43%
- Improve brand reputation – 43%
- Stay competitive and meet customer expectations – 39%
- Prevent mass outages or disruptions caused by third-party incidents – 38%
- Comply with regulations to avoid penalties – 38%

Only further down the list do more traditional financial levers appear, such as lower financial risk, reduced insurance costs and winning new business. That shift in motivation is important: security and compliance are being framed as a route to resilience, customer trust and innovation, and a precondition to growth, not just a line item to placate auditors.

The ROI is real, and measurable

When asked which aspects of their information security compliance delivered the best return over the last 12 months, respondents highlighted a broad range of benefits:

Despite this, fines are still biting, nearly three-quarters received a data protection fine in the last year, with only 26% avoiding penalties. Around half of those fined paid over £250,000. That's a powerful reminder that good intentions without consistent execution still carry a high price.

How long compliance actually takes

This sector is deeply engaged with major standards and regulations. For ISO 27001, ISO 27701, ISO 42001, SOC 2, NIS 2 and GDPR, most organisations achieved compliance in three to nine months, or took up to two years for more complex regimes.

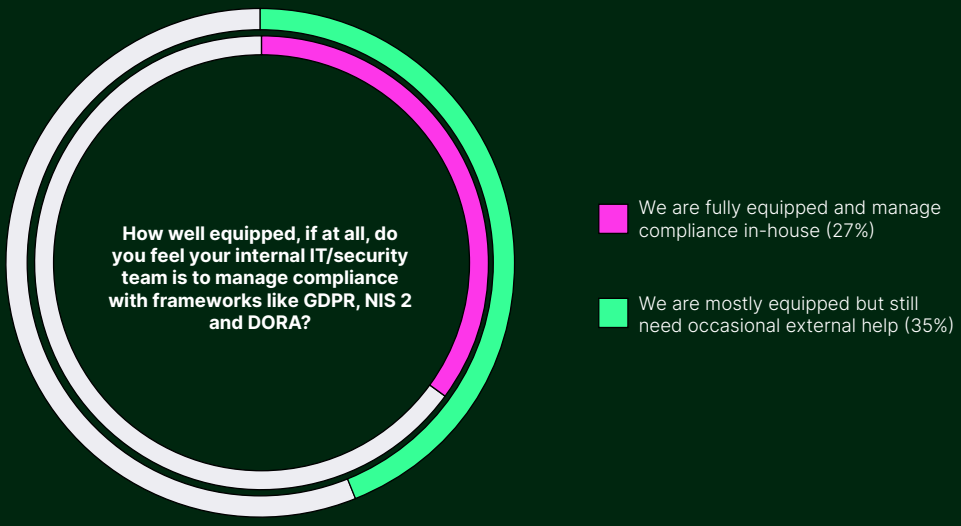
Cost and complexity remain pain points. For ISO 27001 alone, respondents cite:

- Constant changes in regulations (26%)
- High cost of compliance (25%)
- Lack of skilled personnel (21%)
- Lack of clear regulatory guidance and conflicting requirements (19% each)

At the same time, 20% report "no challenges", suggesting that organisations with more integrated, systematised approaches are already breaking out of the compliance crunch.

Internal Teams vs External Support

When it comes to managing overlapping frameworks such as GDPR, NIS 2 and DORA, a minority feel genuinely self-sufficient:



That leaves almost four in ten organisations operating with some kind of structural deficit, whether that's a lack of specialist expertise, limited time alongside BAU workloads, or insufficient board-level backing to do the job properly.

For these teams, the challenge isn't simply "more work". It's that compliance is being bolted on around existing duties, handled in spreadsheets or ad hoc tools, and pushed forward by a small number of overstretched specialists. In that context, it becomes very hard to:

- Keep pace with regulatory changes across multiple regimes
- Apply controls consistently across services, regions and suppliers
- Evidence compliance in a way that stands up to audit or regulatory scrutiny

This is where repeatable processes, shared data and common tooling become critical. Rather than relying on individual heroes or one-off projects, organisations need a way to:

- Centralise obligations and controls across GDPR, NIS 2, DORA and sector standards
- Reduce manual duplication of effort between security, legal, ops and commercial teams
- Give leadership a single, trusted view of where they stand and where the gaps are

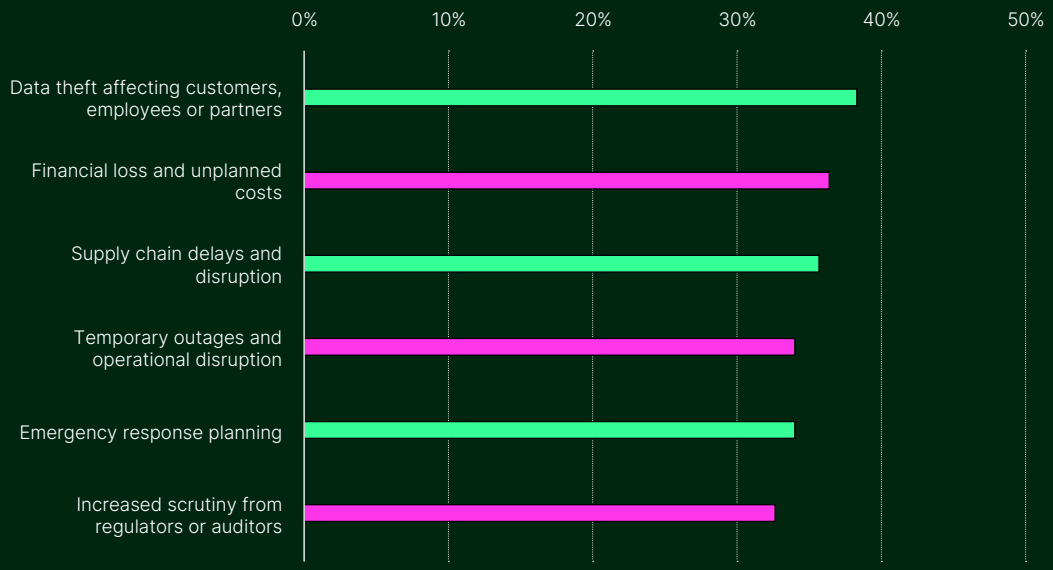
For the sizeable cohort that currently lacks time, skills or support, the priority is less about "doing more" and more about doing compliance differently, moving from reactive, person-dependent activity to a structured system that internal teams and external partners can all work within.

Supply chain fragility and supplier scrutiny

Given their role as suppliers to others, it's notable how actively IT and MSP organisations now scrutinise their own partners.

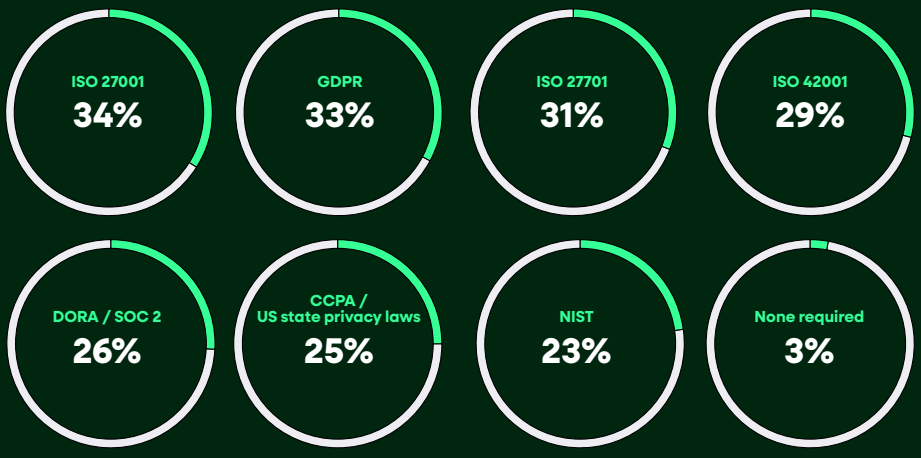
Two-way dependencies

As we previously touched on, 66% have suffered an incident caused by a third-party vendor or partner in the last year. The repercussions are wide-ranging:



In the last 12 months, has your business been impacted because of a cybersecurity/ information security incident caused by a third-party vendor or supply chain partner?

In parallel, these organisations are raising the bar for their own suppliers by requiring them to have certification to;



Which information security standards or regulations, if any, do you require of your suppliers to do business with them?

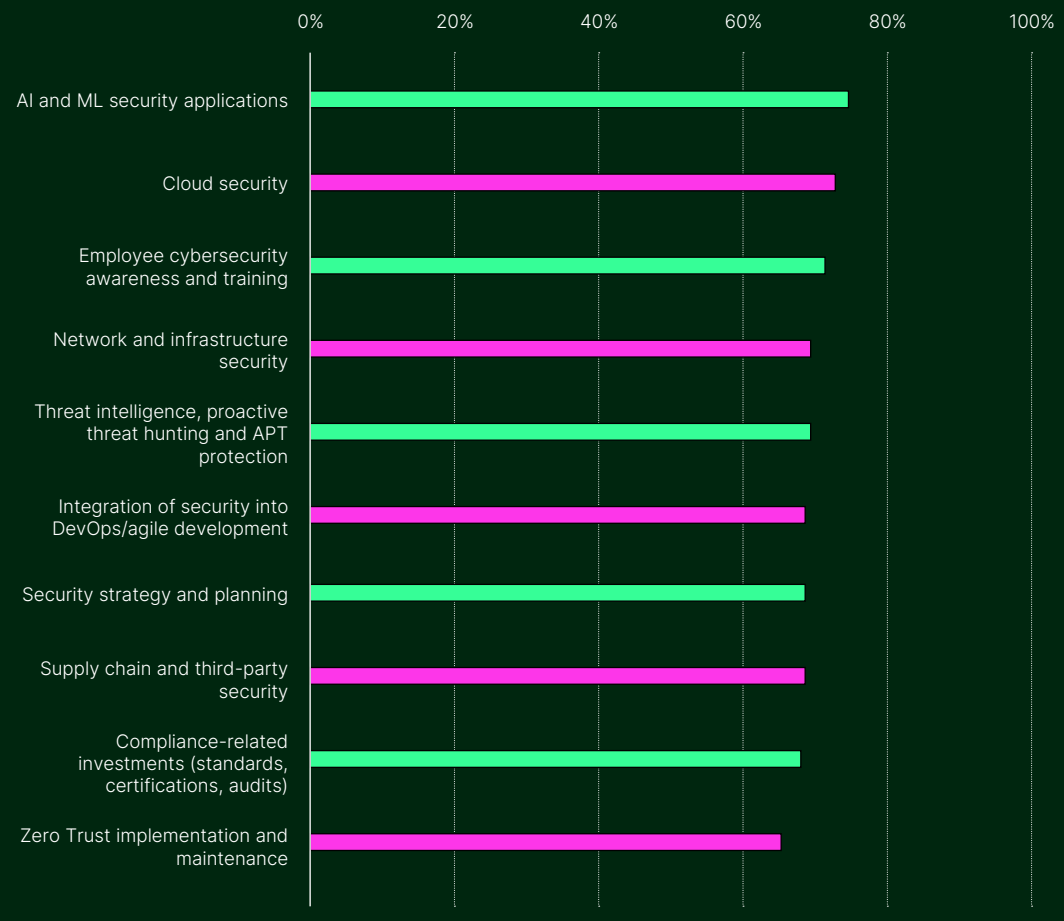
This two-way pressure is gradually driving more consistent controls across digital value chains. But it also adds another layer of complexity for internal teams to track, align on, and evidence – again pointing to the need for unified ways to manage obligations, risks, and supplier data.

Investment outlook: building the next wave of resilience

If there's one area where the sector is not hesitating, it's investment. Across almost every category, they plan to increase information security spend, often significantly.

Where the money is going

Significant or moderate spending increases (over 25% or up to 25%) are planned in:



How, if at all, do you expect your company's information security spend to change in the next 12 months, in the following areas?

There is also a clear appetite for forward-looking capabilities. On top of general quantum-related security spend, 94% plan to invest in quantum risk readiness, and 90% in homomorphic encryption. Security-by-design DevOps practices are another priority, with 95% planning investment.

Outsourcing remains a vital lever too: 62% will increase spending on external security services and operations.

From ad hoc tools to integrated capabilities

The pattern is clear: this sector is transitioning from tactical point solutions towards more integrated, strategic capabilities. Spending is flowing into:

- Architectures (Zero Trust, security-by-design in DevOps)
- Systematic controls (encryption, access management, incident response, governance)
- Organisational enablers (training, strategy, visibility to leadership)

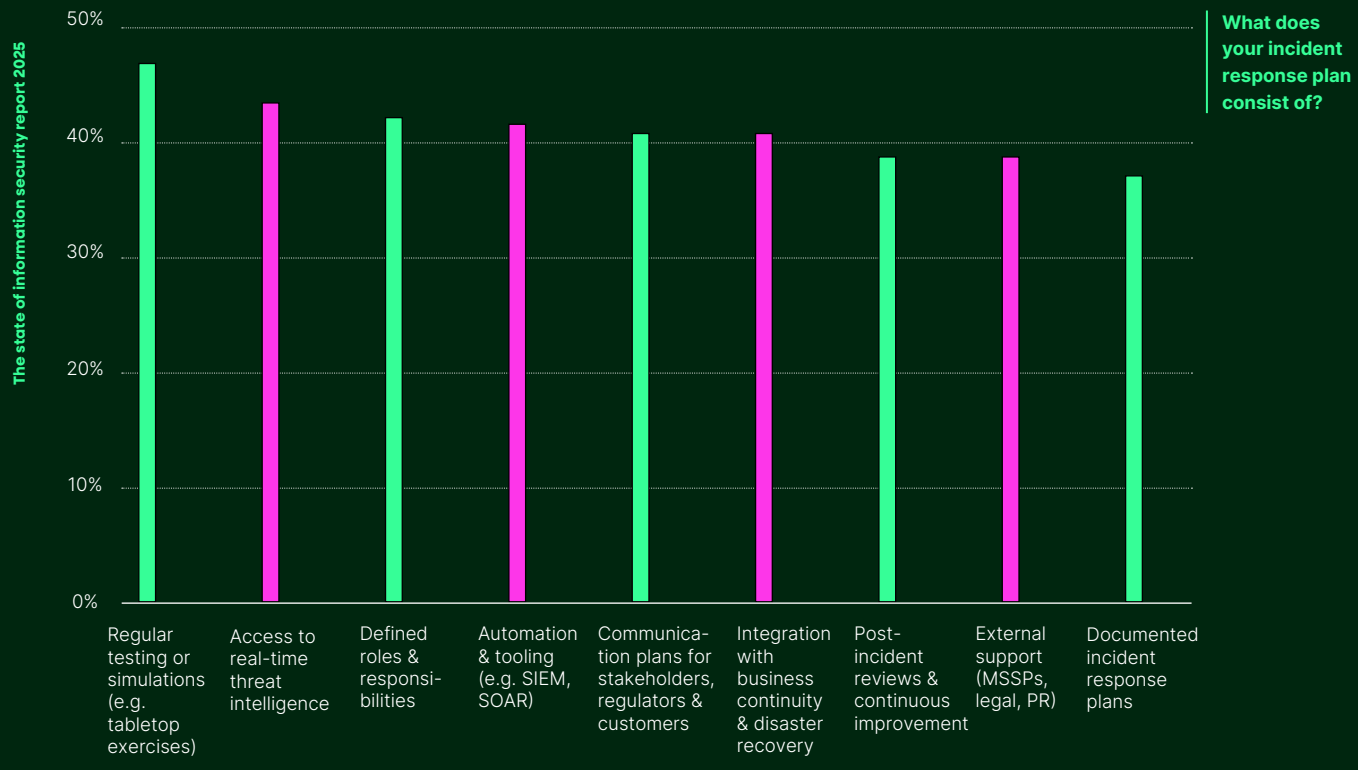
Done well, this kind of investment doesn't just harden defences. It creates a stable operating model for security, something closer to a management system than a toolkit. That's what allows security teams to scale, suppliers

Incident response and resilience: confident, but tested

Few sectors rehearse for crisis as much as IT and MSPs, and it shows.

Prepared on paper, and increasingly in practice

Among those confident in their ability to respond to a significant incident, incident response capabilities typically include:



It's a strong foundation. Combined with the high levels of AI threat preparedness reported earlier, this explains why confidence is so high.

The question now is less "do we have a plan?" and more "how consistently is it embedded?" As the data on post-breach communication failures, process confusion and morale shows, the gap between documentation and day-to-day reality can still be significant.

The road ahead – where the sector is heading

This year's findings tell a clear story about the direction of travel for IT and MSP security leaders.

1. Security is now treated as a strategic enabler.

Motivations and ROI data show that leaders increasingly see information security and compliance as ways to support innovation, customer trust, market access and better decision-making – not simply as insurance against fines.

2. AI has become both the primary risk and the primary lever.

The sector is rapidly building AI-specific defences and governance, while also grappling with the organisational impact of fast adoption, blurred roles and shadow AI.

3. The real bottleneck lies in people and process.

Skills gaps, burnout, leadership ambivalence and employee behaviour remain persistent constraints. Even well-funded programmes will struggle without consistent processes and clear accountability.

4. Supply chain expectations are hardening.

Organisations are both exposed to and driving stricter requirements across their ecosystems. This underscores the need for coherent approaches to tracking third-party risk and compliance, rather than scattering responsibilities across siloed teams and tools.

5. Investment is rising – but will only pay off if it is joined up.

Nearly every major area of security spending is increasing, often significantly. To avoid recreating the tech sprawl that leaders are already struggling with, these investments need to be coordinated, governed and continuously improved as part of a single, coherent approach.

Across every insight, one theme stands out: **the sector is moving away from reactive, tool-driven security towards integrated, repeatable security management systems**. Organisations that can align their people, processes, technologies and obligations in a single operating model will be best placed to:

- Absorb AI-driven threats
- Navigate overlapping standards and regulations
- Demonstrate resilience to customers, regulators and partners
- Turn security and compliance into a genuine commercial advantage

For IT, MSP and telecoms leaders, the challenge now is not whether to invest in information security, that decision has already been made.

The challenge is to ensure those investments are orchestrated, measured and continuously refined within a structured framework that keeps pace with the services they deliver and the ecosystems they support.

Get the full story in

The state of information security report 2025

Read the full report →

Explore more at **isms.online**