Public V1.0

The state of information security report 2025

The state of information security report 2025

About the author

Phil Muncaster has been an IT journalist for 15 years. He started out as a reporter on enterprise IT title IT Week in 2005 and progressed to the role of News Editor before leaving to pursue a freelance career. Since then, Phil has written for titles including The Register, where he worked as Asia correspondent whilst based in Hong Kong for over two years, MIT Technology Review, SC Magazine, Infosecurity Magazine and others.

About io

At IO, we believe compliance should fuel progress, not hold it back.

That's why we built a modern platform to simplify, strengthen, and scale information security, privacy, risk and AI management. Supporting 100+ global standards, including ISO 27001, ISO 27701, ISO 42001, GDPR, and NIS 2, IO gives teams everything they need to stay secure, aligned, and audit-ready in one place.

Our approach blends people, process, and platform, because lasting compliance isn't achieved by automation alone. With guided support, structured workflows, and smart integrations, IO embeds compliance into daily operations—reducing duplication, surfacing insights, and building confidence.

Trusted by thousands worldwide, IO turns compliance from a box-ticking chore into a strategic advantage.

Foreword

As businesses embrace cloud, AI, and digital transformation, the risks grow just as fast. Our State of Information Security Report 2025 reveals how organisations are adapting, where gaps remain, and what resilience looks like in the year ahead.

Chris Newton-Smith

CEO

io

The reality is that threats will keep changing. What matters is that we are better prepared, treating information security not as a back-office function, but as part of how we build resilience, earn trust and grow.

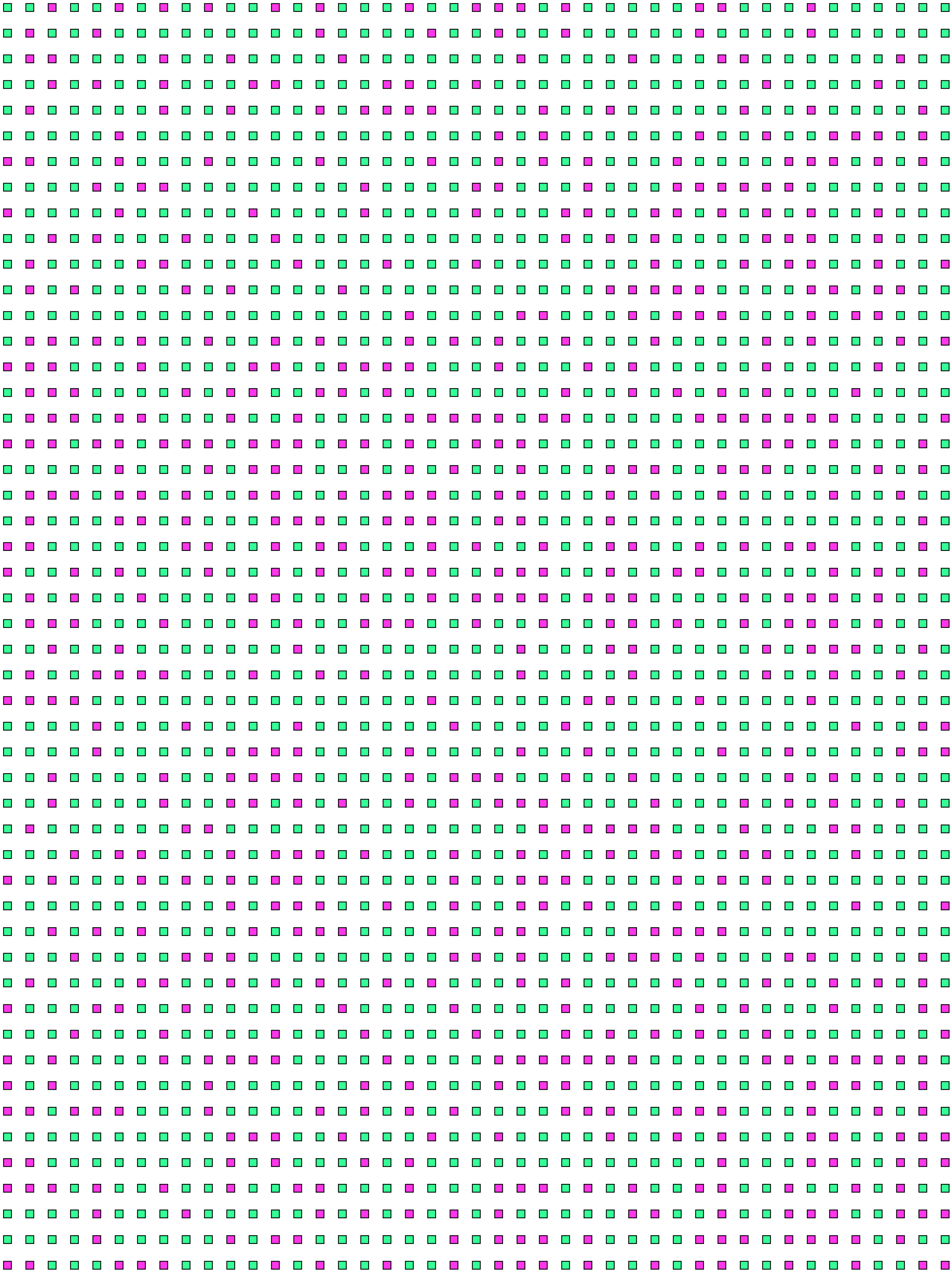
Over the past year, we've seen organisations double down on digital change, rolling out cloud services, experimenting with AI, and adopting new tools to stay ahead. But with each step forward comes added exposure. The attack surface keeps expanding, and attackers are quick to take advantage.

Our State of Information Security Report 2025, based on insights from over 3,000 professionals across the UK and US, shows just how complicated this picture has become. Ransomware is still with us, but criminals are increasingly turning to data theft and extortion. Phishing and malware remain daily frustrations, and misconfigured cloud systems continue to create easy openings. At the same time, AI is proving to be both a powerful asset and a new source of risk, with shadow AI and data poisoning high on the list of emerging concerns.

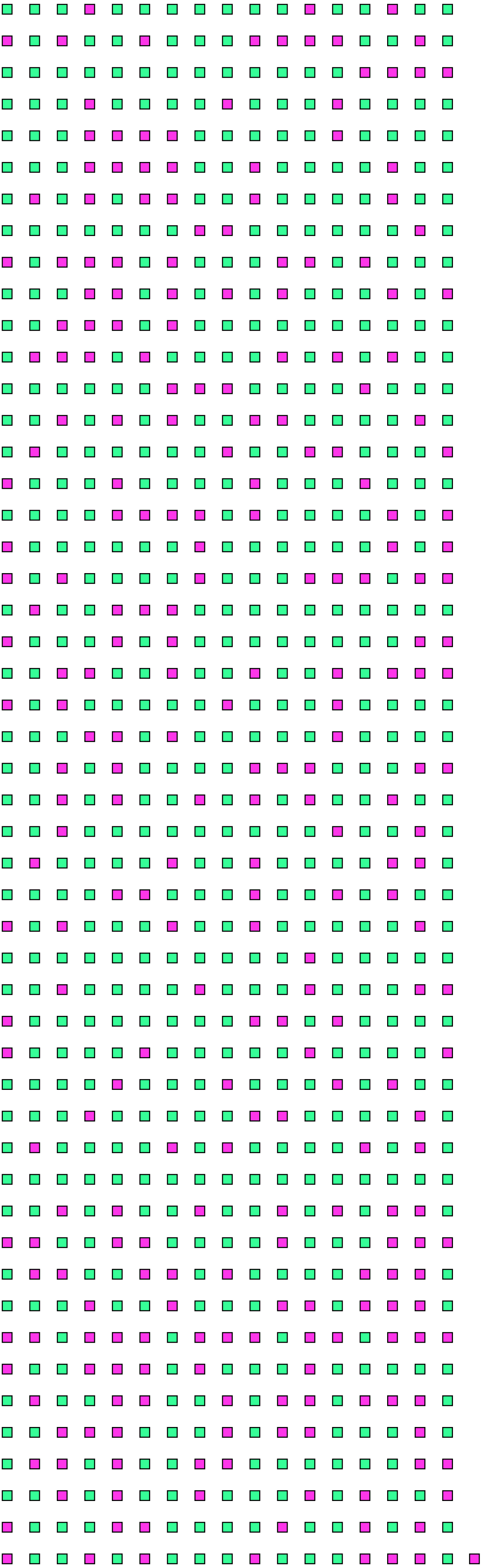
The financial impact is also hard to ignore. Last year, 71% of organisations received fines, and almost a third of those penalties were more than £250,000. What's striking, though, is the shift in how businesses now view compliance. Rather than simply treating it as a way to avoid fines, more firms are using frameworks such as ISO 27001 and SOC 2 to strengthen trust, sharpen decision-making, and even open up new commercial opportunities.

The people challenges haven't gone away. Skills shortages, staff burnout, and awareness gaps remain stubborn problems. But there are real signs of progress: boards are paying closer attention, budgets are increasing, and organisations are moving away from firefighting towards building resilience. Three-quarters of respondents told us they feel more confident about security than they did a year ago, and almost all believe they could respond effectively to a major incident.

The reality is that threats will keep changing. What matters is that we are better prepared, treating information security not as a back-office function, but as part of how we build resilience, earn trust and grow. I encourage you to explore the full report and take a closer look at these and many other risks facing businesses today. We hope you enjoy reading and look forward to the important conversations it will start.



The state of information security report 2025



About the research

ISMS.online commissioned leading independent market research firm Censuswide to help us better understand the current information security and compliance landscape. Unlike last year's report, which canvassed the opinions of respondents from the US, UK and Australia, this year we polled 3,001 respondents who work in information security across the UK (2,000), and US (1,001).

Their responses have helped us to uncover the main information security and compliance challenges facing organisations in these regions, and particularly the impact of AI on the landscape. We thank them for their invaluable input.

Makeup of total respondents from this year's survey

🟩 UK respondents (2,000)

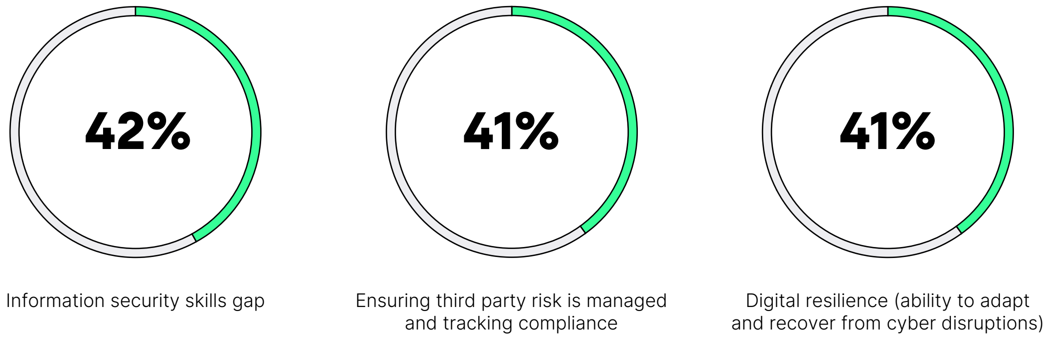
🟪 US respondents (1,001)

01

The attack surface continues to grow

As organisations double down on digital transformation, their attack surface continues to expand. In 2025, the challenge is no longer just transformation, but balancing innovation with resilience in the face of relentless cyber threats.

What are the main challenges facing your business (top responses)



Last year, we spoke about the catch-22 situation many organisations are finding themselves in. On the one hand, the push for digital transformation is vital to carve out competitive advantage, improve customer experiences and streamline business processes. But at the same time, these efforts expand the cyber-attack surface, providing more opportunities for threat actors to strike.

If anything, these trends are even more pronounced in 2025, as organisations double down on digital amid persistent economic and business uncertainty, and adversaries take advantage. It's why many respondents cite things like securing emerging technologies (39%), cloud services/apps (37%) and IoT/BYOD (28%), as well as managing third-party risk (41%), among their top challenges. Tech sprawl (35%) resulting from too many siloed point solutions also signifies anxiety over the size of the attack surface. As does the fear of "as-a-service" cyber threats like ransomware-as-a-service (39%), which are democratising the means to compromise corporate networks via under-protected endpoints.

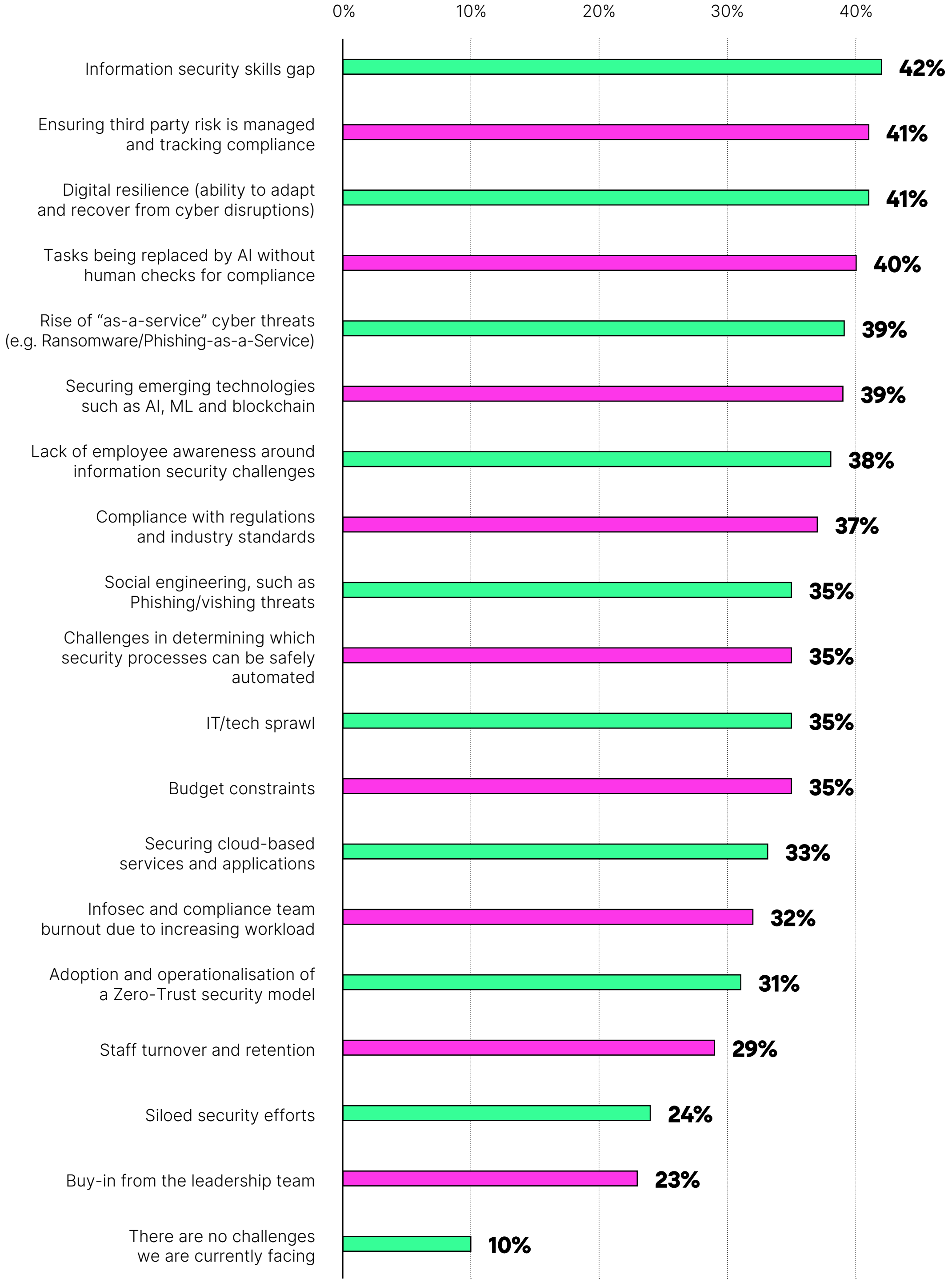
The global workforce gap in cybersecurity now stands at nearly 4.8 million. AI will be able to absorb some of this shortfall. But even it needs skilled professionals to deploy, manage, train and interpret output.

But the attack surface isn't just comprised of technology solutions. As we'll discuss later in the report, it's also distinctly human in parts. A lack of employee awareness, cited as a challenge by 38%, can lead directly to successful social engineering attacks (35%) and compromise. Employees are also bypassing officially sanctioned and managed technology solutions. Shadow AI is one of the biggest emerging concerns for the year ahead, cited by 37% of respondents. And shadow IT (40%) is described as the most common employee security "mistake" of the past year.

Even more acute is the persistent skills gap in cybersecurity teams, cited by 42%. According to ISC2 figures, the global workforce gap in cybersecurity now stands at nearly 4.8 million professionals, including over

392,000 in Europe and almost 543,000 in North America. AI will be able to absorb some of this shortfall. But even it needs skilled professionals to deploy, manage, train and interpret output.

Against this backdrop, many (37%) organisations are struggling to comply with industry regulations and standards. The former is concerning, given the potentially significant financial penalties that can now be levied by regulators. The latter is disappointing, as best practice standards like ISO 27001 can actually help to reduce the regulatory compliance burden, given many new pieces of legislation – especially in Europe – require similar foundational steps be put in place.



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

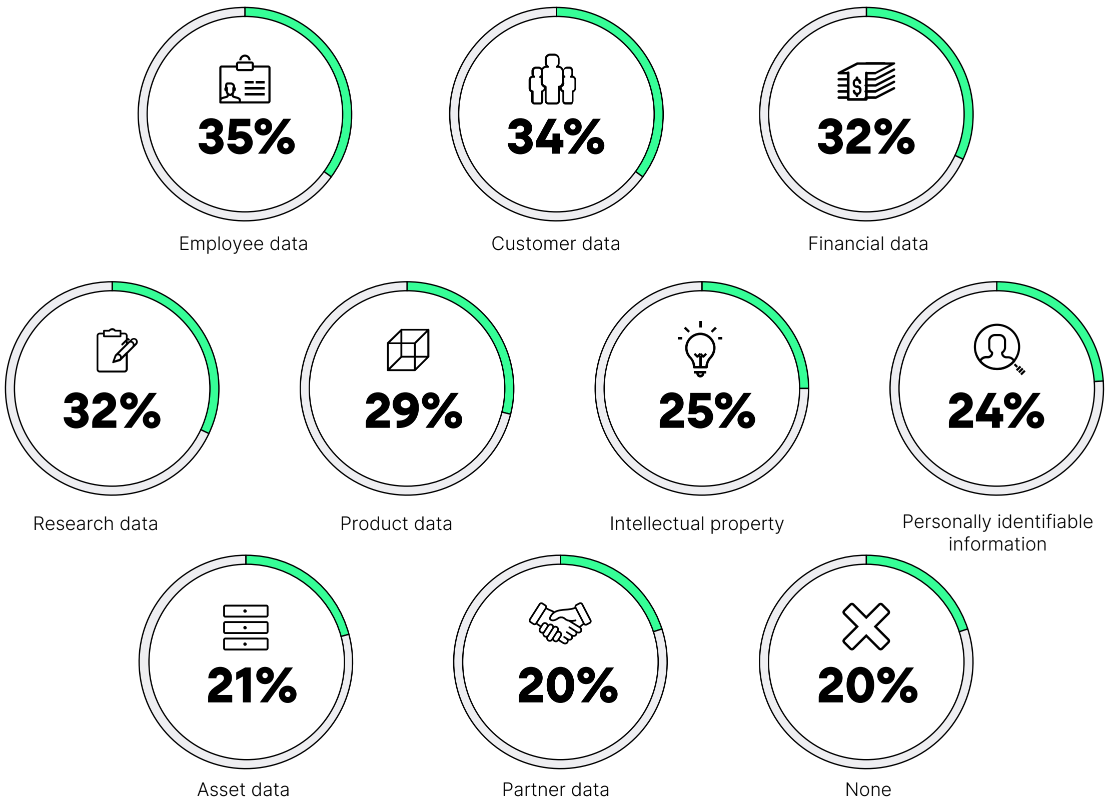
The resilience challenge

A final challenge worth mentioning is digital resilience, cited by 41% of respondents. As ransomware and data extortion attacks cause chaos on both sides of the Atlantic, it has become increasingly important to company boards and stakeholders that organisations can continue to operate, even following a breach. The concept lies at the heart of regulatory efforts like DORA and NIS2.

However, IBM claims that 86% of data breach victims over the past year experienced operational disruption affecting customer-facing services, sales processing and production. Given today's regulatory context, the consequences of such failings could be even more severe. Our data reveals that only 29% of organisations weren't fined for data breach violation last year, with 30% experiencing fines of over £250,000. The good news is that, despite the relatively large share of our respondents citing challenges achieving digital resilience, many are moving in the right direction. As we'll see, the threat landscape is undeniably weighted in the favour of our adversaries. But by assuming breach and preparing for the worst – through incident response, recovery planning, threat intelligence and more – organisations can and are improving resilience.

The threat landscape is undeniably weighted in the favour of our adversaries. But by assuming breach and preparing for the worst – through incident response, recovery planning, threat intelligence and more – organisations can and are improving resilience.

Which types of data have been compromised in your organisation in the past 12 months?

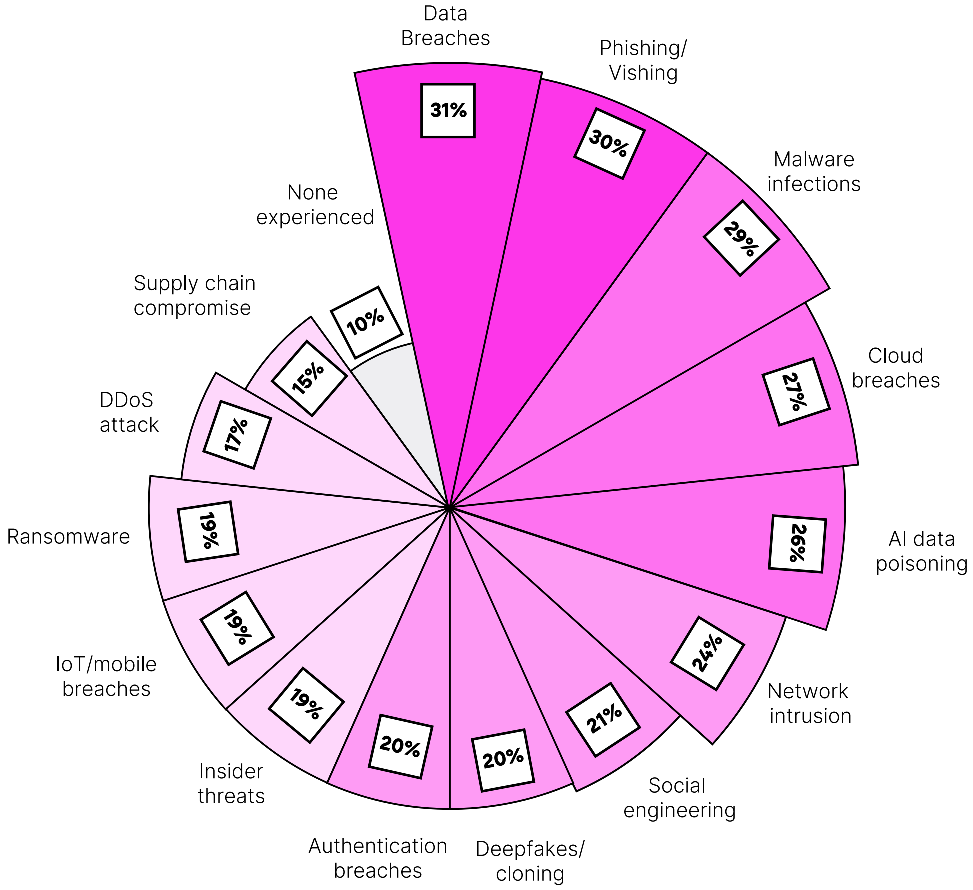


02

Emerging threats dominate the landscape

The threat landscape continues to evolve rapidly, shaped by both criminal and state-aligned actors. From ransomware and data breaches to AI-driven attacks, organisations face a complex mix of risks that are driving up cost and disruption.

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



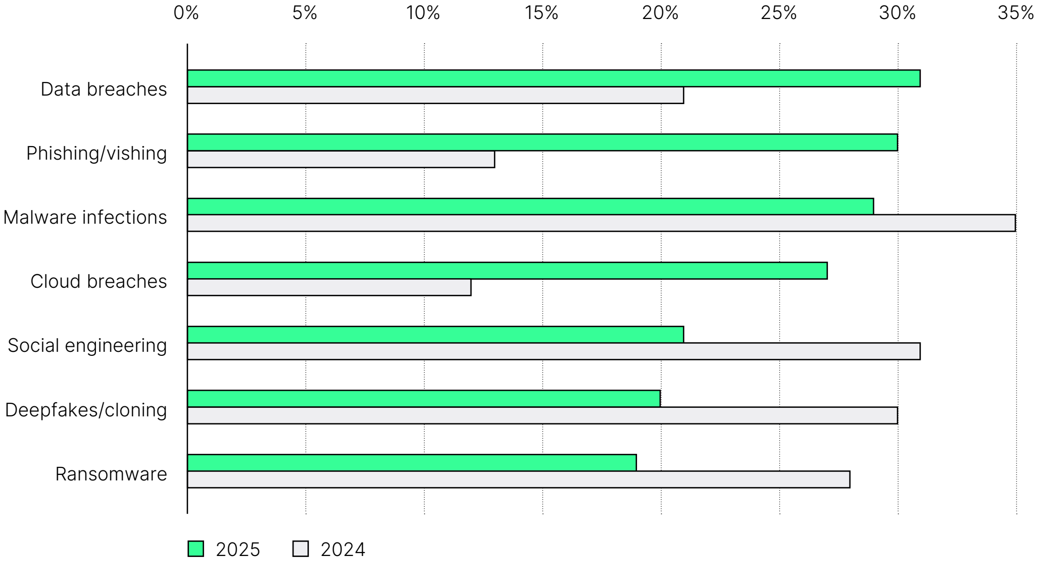
Over the past year, we've seen the threat landscape do what it does best: evolve at breakneck speed in response to technology innovation and the changing demands of its participants. These individuals may be financially motivated cybercriminals or state-aligned actors. Increasingly, the lines between the two are blurring, as states hire cybercrime groups, use their tooling for plausible deniability, and allow state actors to moonlight.

But whatever the motivations of threat actors, we've seen a number of trends start to coalesce in recent months, with major implications for network defenders. They are reflected in the most common cybersecurity events experienced by our respondents over the past 12 months. These include:

Ransomware (19%): Notably less prominent than last year (29%), but still a menace. We know that organisations are less likely to pay the ransom these days. A blockchain analysis reveals a 35% annual decline in the value of ransomware-related crypto payments in 2024 – a figure that may fall further if UK government proposals to ban payments from some organisations takes effect. However, unpatched vulnerabilities, phishing and compromised credentials are widespread enough to give threat actors plenty of targets.

Data breaches (31%): The ransomware epidemic is likely to contribute to the large share of respondents suffering data breaches last year. In many cases, threat actors are forgoing the ransomware deployment altogether in favour of simpler data theft extortion attacks.

Malware infections (29%): This figure is surely fuelled by a tremendous uptick in the number of infostealer attacks, which in turn is providing a steady dark web supply of compromised credentials for initial access and lateral movement. One estimate claims that 75% (2.1 billion) of 3.2 billion credentials stolen in 2024 were taken via infostealers.



Year-on-year comparison for types of cybersecurity/ information security incidents has your business experienced 2024 vs 2025

The benefit for threat actors is that using a stolen credential for access avoids setting off any alarms. Routes to infection include malvertising, drive by downloads, mobile apps, and phishing.

Social engineering (21%) and phishing (30%): This is a major enabler for ransomware, data breaches and infostealer successes. A relatively recent trend has been of native English speakers (aka ShinyHunters, Scattered Spider) using vishing techniques impersonating or targeting the IT helpdesk in order to obtain corporate credentials. This has led to a spate of ransomware attacks and data breach extortion attempts (targeting Salesforce CRM databases).

Cloud breaches (27%): As more organisations migrate data, infrastructure and applications to the cloud, these environments are coming under greater threat actor scrutiny. Infostealers and phishing can explain some of this figure (see above targeting of Salesforce SaaS accounts). Alternatively, hackers can quite easily take advantage of misconfigured cloud instances by scanning en masse with automated tools.

The AI threat: Deepfake-powered attacks (20%) may not be as big a problem as they were last year. But AI data poisoning (26%) has taken their place. These are more advanced attacks capitalising on the trend for homegrown LLM-powered systems, and enabling threat actors to sabotage models, create backdoors and achieve other nefarious goals.

AI threats also dominate respondents' concerns for the coming 12 months; most obviously AI-generated mis- and disinformation (42%). This is usually a nation state threat, although cybercriminals could also use fake news to promote scams on hijacked corporate social media feeds, impacting reputation. Generative AI (GenAI) is a highly capable tool for generating social engineering campaigns at scale (38%).

Respondents also cite unsanctioned use of AI (34%), and deepfakes used during virtual meetings (28%). The latter could involve business email compromise (BEC) attempts, or even fraudulent attempts by North Korean IT workers to gain employment. IT security managers are also concerned about deep-

In total, only 29% say they did not receive a fine for a data breach or violation of data protection rules in the past 12 months. Clearly, much work still needs to be done to improve compliance efforts.

fake cloning more generally (27%), which is increasingly being used by threat actors to impersonate customers and bypass KYC checks.

AI threats could also be contributing to concerns about supply chain breaches and geopolitical threats (both 23%).

Counting the cost

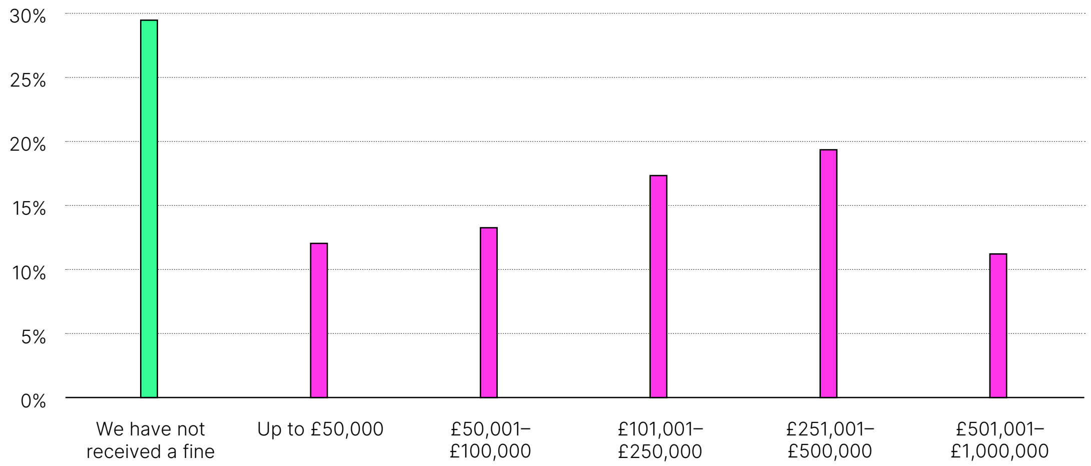
These concerns are often based on experience. Our interviews reveal around a third of British and American organisations have had employee (35%), customer (34%), financial (32%), research (32%) and product (29%) data compromised over the past year, as well as IP (25%). Only a fifth (20%) say that no data loss occurred in the period.

Depending on the type of data breached, this can have a significant impact on the victim organisation – ranging from employee termination to customer churn, system downtime, legal action and increased partner scrutiny.

The financial cost can also be significant, including that stemming from supply chain disruption, remediation, notification, internal investigations, loss of competitive advantage, and regulatory fines. Some 19% of respondents claim they were fined between £251,001–£500,000, while a further one in 10 (11%) were fined over £501,000 during the past year. Over two-fifths (41%) were fined up to £250,000.

In total, only 29% say they did not receive a fine for a data breach or violation of data protection rules in the past 12 months, meaning 71% did. Breach incidents also led to disciplinary action and terminations (33%), internal investigations (31%), loss of competitive advantage (18%) and business closure or a strategic pivot (18%). Clearly, much work still needs to be done to improve compliance efforts.

What is the total amount your business has received in fines for a data breach or violation of data protection rules in the last 12 months?

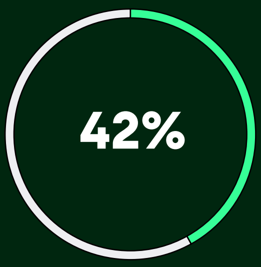


03

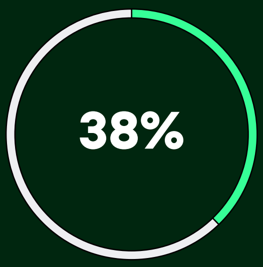
The AI threat and opportunity

AI is increasingly shaping the information security landscape. It introduces risks such as shadow AI, data poisoning and malicious use, while at the same time offering defenders new ways to strengthen resilience and close critical skills gaps.

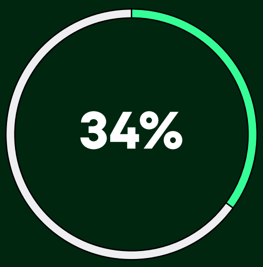
What are your biggest emerging threat concerns for the next 12 months?



AI-generated misinformation and disinformation



AI phishing



Internal misuse of generative AI tools (“shadow AI”)

As per last year, AI is both a cause of many cybersecurity problems, and part of the solution. The challenge comes in two parts: AI-powered threats like deepfakes and GenAI-driven phishing on the one hand, and exploitation of AI infrastructure like data/ model poisoning on the other.

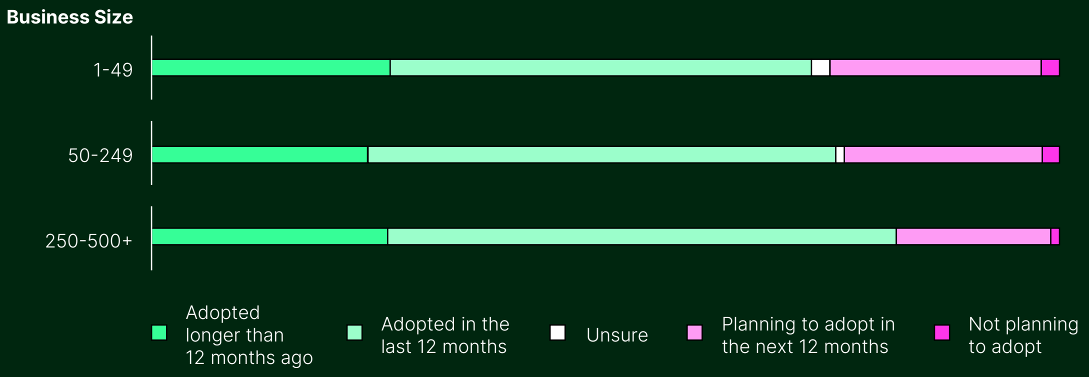
The latter risk category, which also includes theft of training data, continues to grow as businesses expand their use of AI. Call it the growth of the AI attack surface. Some 79% of respondents say they have adopted new technologies like AI and machine learning (ML) in the past 12 months, with a further 19% planning to do so in the next 12. Small businesses (73%) are less likely to have deployed the tech already than their larger peers (81%), but more likely to be planning adoption (21% vs 17%).

11% of breached organisations claim not to be sure if they experienced a shadow AI incident, which means that they probably did.

The big danger is not planned adoption, but so-called “shadow AI”: unmanaged use of the technology. While this could refer to unsanctioned use of agentic AI, in our case it’s all about GenAI. A third (34%) of respondents claim to be concerned about the risk. They’re right to be. IBM claims that shadow AI-related incidents accounted for 20% of breaches over the past year. An additional 11% of breached organisations claim not to be sure if they experienced a shadow AI incident, which means that they probably did. Some 37% of our respondents claim employees are using GenAI without permission.

Shadow AI presents several risks. First, employees may share sensitive information including IP or customer data with a public GenAI tool, which could theoretically

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?



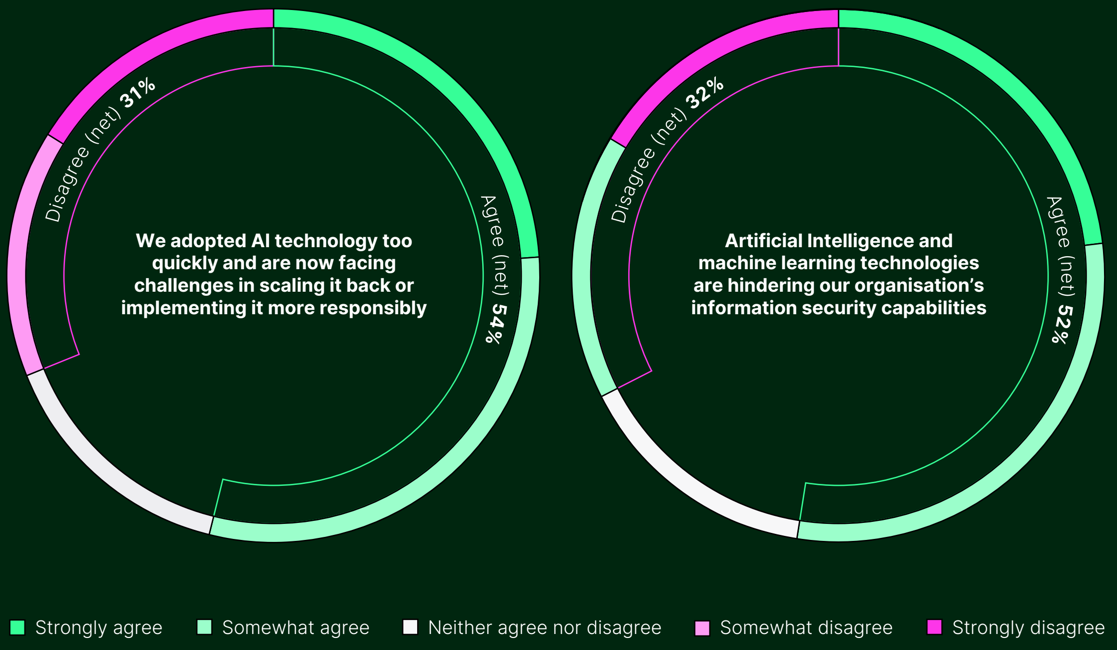
regurgitate it back to other users. This raises serious GDPR compliance concerns. The data shared with such a tool may also be breached by hackers, or accidentally leaked by the AI company itself, as happened with Chinese firm DeepSeek. The GenAI tools being used by employees might also contain vulnerabilities, silently expanding the AI attack surface.

Given the risks, it's somewhat disappointing that only a fifth (21%) of respondents cite "establishing or enforcing responsible AI usage policies" as a priority for the coming year. However, there's a balance to be struck. More than half (54%) of respondents claim they adopted AI technology too quickly and are now facing challenges in scaling it back or implementing it more responsibly. Moving too fast might break things. But not fast enough and employees may find insecure workarounds. Fortunately, 95% are investing in AI governance and policy enforcement.

Moving too fast might break things. But not fast enough and employees may find insecure workarounds.

The other big category of AI threats is, of course, those driven by malicious use of the technology. The UK's National Cyber Security Centre (NCSC) warns that over the next two years, "AI will almost certainly continue to make elements of cyber intrusion operations more effective and efficient, leading to an increase in frequency and intensity of cyber threats." Alongside social engineering, it cites AI assisting threat actors in malware generation, data exfiltration and vulnerability research and exploit development (VRED).

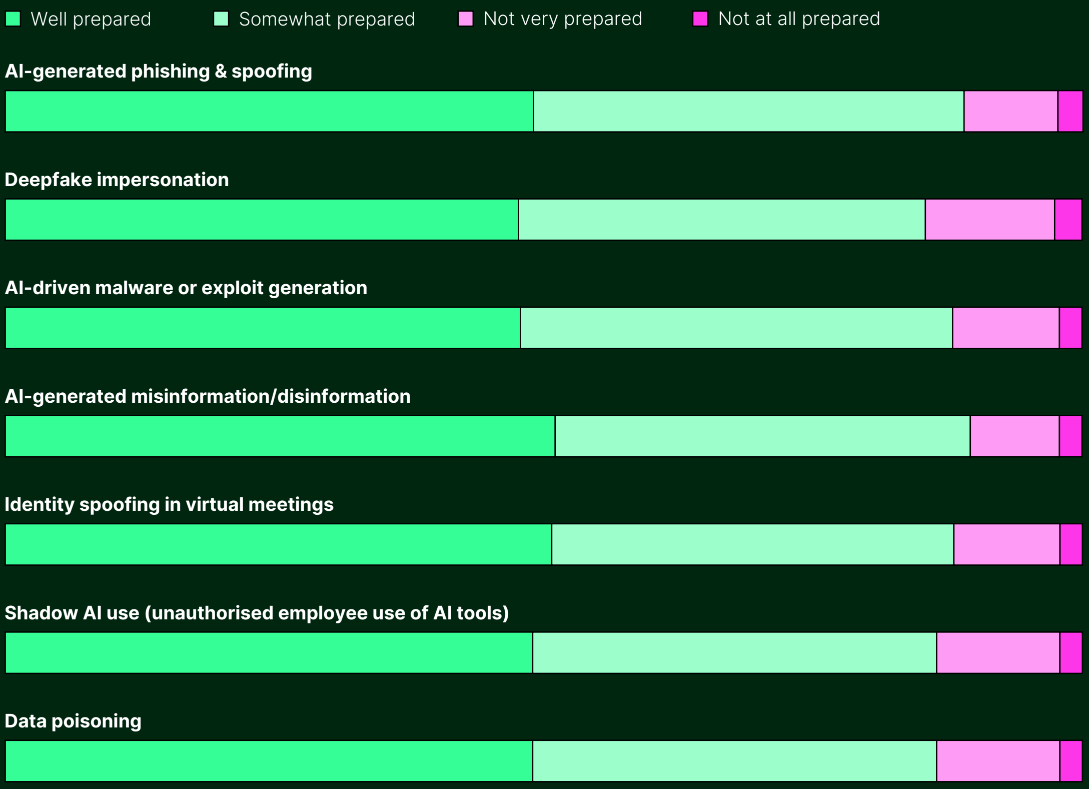
That's why it's reassuring that the number one cybersecurity priority for respondents over the next 12 months is enhancing defences against AI-generated threats (30%). A quarter also say they will focus on improving their ability to authenticate digital communications and detect manipulation, which could help prevent AI-powered phishing.



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

An overwhelming majority also claim to feel prepared to detect, defend against, and recover from AI-generated threats. If their confidence is justified, respondents' ongoing efforts to enhance resilience are already in a good place.

How prepared, if at all, is your organisation to detect, defend against, and recover from the following AI-driven threats?



AI for threat defence

Another reason to be cheerful is the potential benefits of AI-powered cybersecurity tools. AI is being built into just about every type of security product today, and while there's plenty of hype, there are also some proven use cases. AI algorithms can trawl through vast datasets to surface signals of suspicious behaviour for SecOps teams to investigate. GenAI assistants can help teams close skills gaps in understaffed areas like SOC analysts. It can also improve malware and phishing detection, automate toilsome tasks for security teams, and even help to spot malicious use of AI.

It's reassuring that the vast majority (96%) of respondents plan to invest in GenAI-powered threat detection and defence, and deepfake detection and validation tools (94%). A further 30% say they're prioritising the improvement of defences against AI-generated threats. And a quarter (25%) are planning a 25%+ increase in security spending on AI/ML security apps. An overwhelming majority also claim to feel prepared to detect, defend against, and recover from AI-generated threats like phishing (89%), deepfakes (84%), AI-driven malware (87%), disinformation (89%), identity spoofing in virtual meetings (88%) and data poisoning (86%).

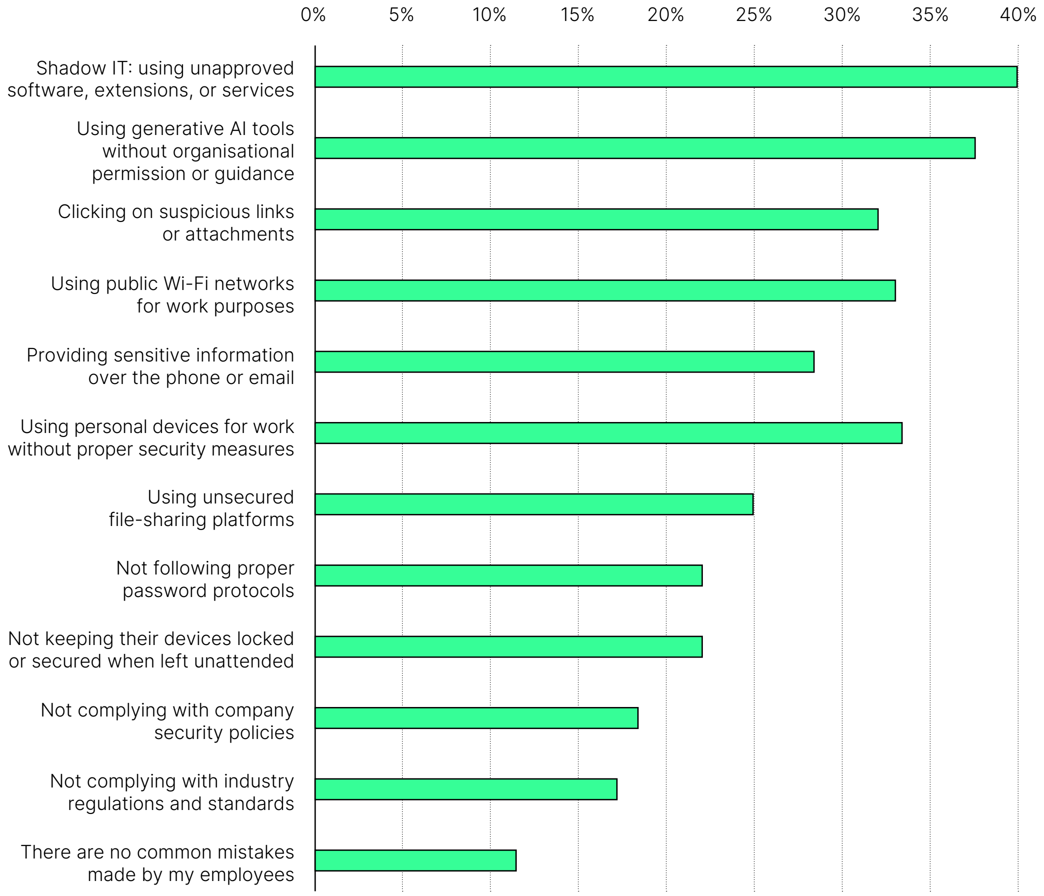
If their confidence is justified, respondents' ongoing efforts to enhance resilience are already in a good place.

04

The people advantage

Humans have sometimes unfairly been described as the weakest link in the corporate cybersecurity chain. In fact, they are simply another cyber risk to be managed. But the risk goes beyond the security awareness (or lack of it) of regular employees.

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

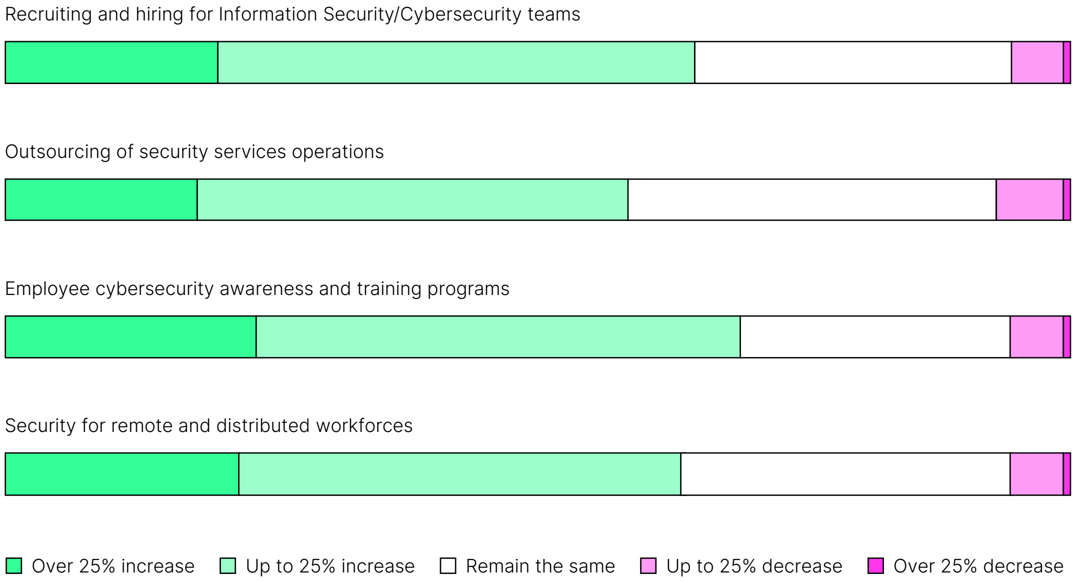


As our research reveals, the people-shaped risk also extends to the cybersecurity team. The information security skills gap is the number one challenge facing British and American respondents today (42%).

The challenge is being compounded by burnout due to increasing workload, cited by a third (32%) of respondents. And staff turnover/retention issues (29%). If more talent ends up leaving the industry, those who remain will be under even more pressure to deliver. The problem is particularly acute in fields such as SecOps, where analysts are often overwhelmed by data and alerts from security point solutions across their environment. This alert overload, a common feature of technical sprawl, means real threats get passed over while analysts waste their time chasing false positives.

Similar challenges can impact compliance teams frustrated by inconsistencies in best practice standards and frameworks, and the sheer volume of diverse regulations in play. It makes compliance a top challenge for 37% of respondents. It also helps to explain why nearly two-fifths (39%) of respondents complain that their in-house team is not equipped to handle compliance with regulations like NIS2, DORA and GDPR.

> ***The challenge is being compounded by burnout due to increasing workload, cited by a third (32%) of respondents, and staff turnover/retention issues (29%). If more talent ends up leaving the industry, those who remain will be under even more pressure to deliver.***



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

People, process and technology

There's no easy solution to these challenges. But our data points to some causal factors that could be worked on. Most obvious is budget shortfalls, cited by 35% as a challenge, and lack of buy in from the leadership team (23%). If CISOs could better master the art of aligning security and business outcomes, and speaking in a language the board understands, they may stand a better chance of securing more budget. There are hints this could already be happening: 64% of respondents say they're increasing budget for infosec recruitment over the coming year – with a fifth increasing by over 25%. Some 58% are also increasing spend on outsourcing, which is another worthwhile option.

Organisations can work smarter to optimise the security work they do. AI could help to reduce manual toil and free staff up to work on higher-value tasks, as well as upskill less experienced members of a team, for example. AI is helping to blur the scope and responsibilities of traditional security roles, according to 67% of respondents. This is fundamentally a positive trend.

On a similar theme, over a third (35%) of respondents cite challenges in determining which security processes can be safely automated. Prioritising this area may help to surface some quick wins for teams. But we also mustn't forget the value of humans in the loop. Two-fifths (40%) of security leaders cite as a challenge tasks being replaced by AI without human checks for compliance.

Separately, investments in platform-based solutions (as opposed to point products) could help to overcome the challenge of

If CISOs could better master the art of aligning security and business outcomes, and speaking in a language the board understands, they may stand a better chance of securing more budget.

siloed security effort, cited by 24%. This often leads to duplicated work, creating security coverage gaps and overspend. It's good to see 16% of organisations consolidating security tools and platforms to reduce complexity. But these numbers could certainly go higher. Standardised processes and share culture/vision can also help remove silos. This hints at the other key takeaway: that only a combination of people, process and technology can solve the cybersecurity challenges linked to employees.

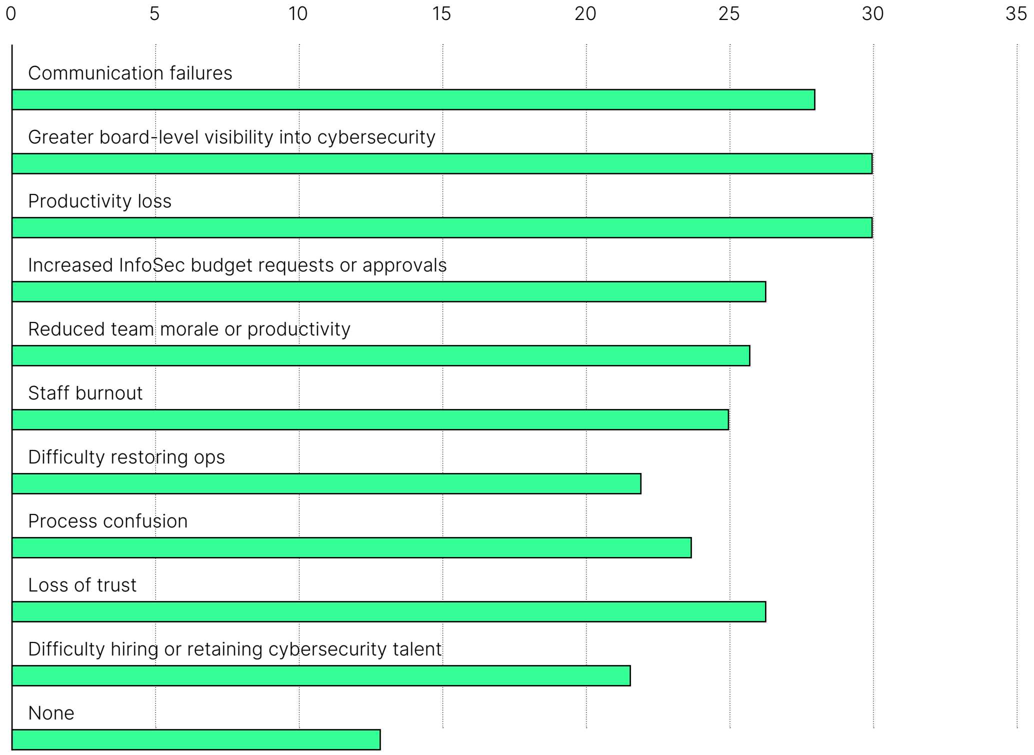
Security awareness training should not just focus on phishing. Such training courses must adapt to new social engineering tactics, like vishing, as well as deepfakes and other AI-related risks.

The employee challenge

The other critical people challenge remains one of security awareness, cited by 38% of respondents. It's part of the reason why so many are experiencing social engineering and phishing incidents. And why shadow AI is an emerging problem. In fact, the top two infosec "mistakes" mentioned by respondents over the past year are shadow IT (40%) and shadow AI (37%). Next comes use of unsecured personal devices for work (34%) – a problem amplified by home and remote working. And use of public Wi-Fi for work (32%).

It's evidence, if any were needed, that security awareness training should not just focus on phishing – although clicking on suspicious links (32%) is also cited as a key infosec mistake. Such training courses must adapt to new social engineering tactics, like vishing, as well as deepfakes and other AI-related risks. And they should be backed by investments in technologies like passwordless security – which has been adopted by 67% over the past year.

What people/ process challenges arose after a breach?

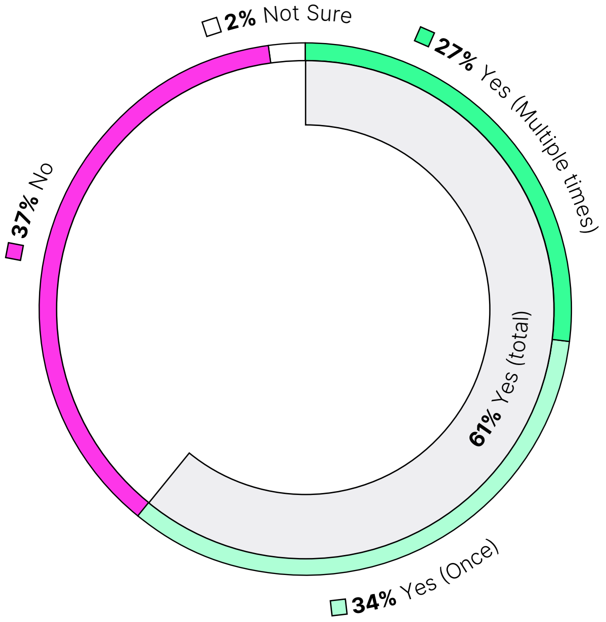


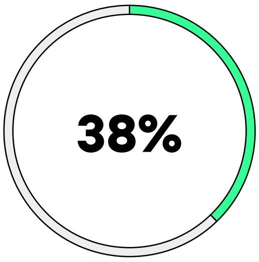
05

Why supplier security matters

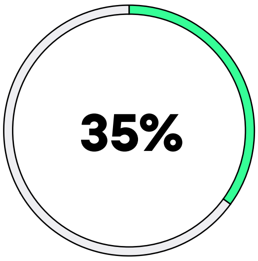
Supply chains are the backbone of modern business, yet they remain a persistent weak point in information security. With new regulations raising the bar, organisations must balance opportunity with the growing risks posed by third-party partners.

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?





Resulted in a data breach affecting customers, employees or partners



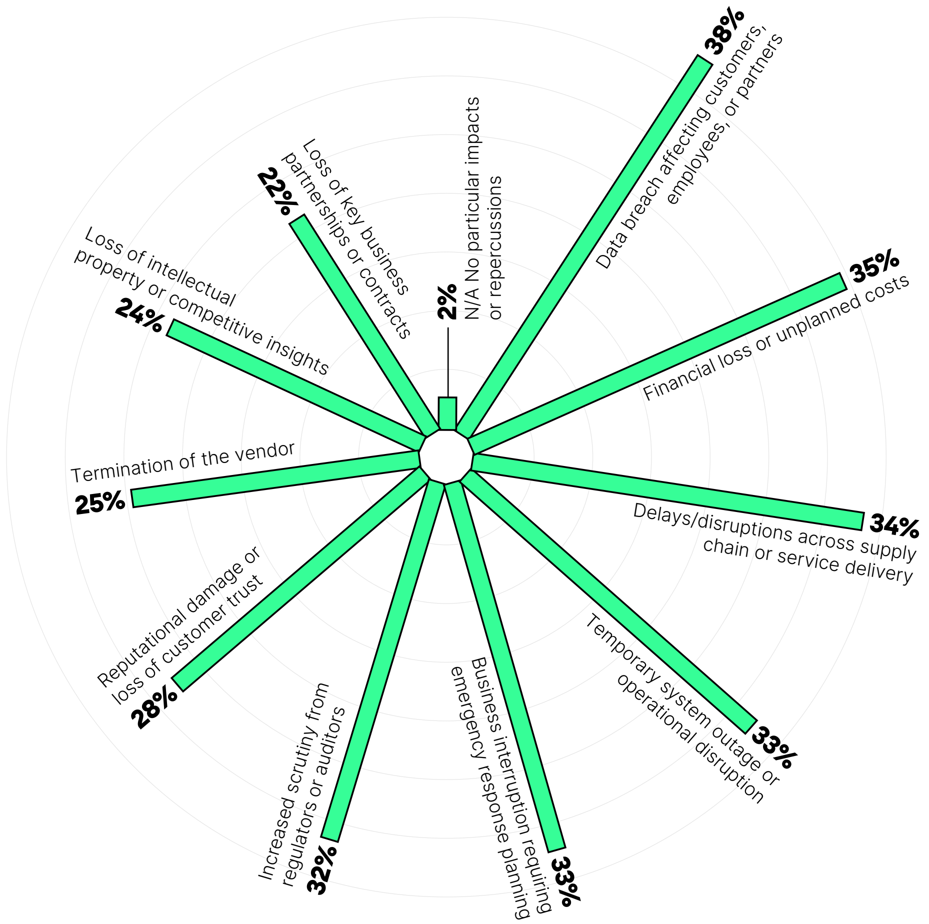
Resulted in financial loss or unplanned costs (eg, remediation, fines, legal fees)

Supply chains remain a critical feature of business operations – from IT helpdesk contractors to professional services firms, MSPs and software developers. They also remain a fundamental weakness that threat actors are past masters at targeting. Yet 41% of respondents admit that managing third-party risk and compliance is a challenge. That's worrying news, especially in light of new regulations like DORA, NIS2 and the UK's Cyber Security and Resilience Bill, which put a stronger emphasis on supply chain risk management.

As if to illustrate this challenge, 61% of respondents admit that their business has been impacted by a security incident caused by a third-party vendor in the past year. Nearly two-fifths (38%) say it led to customer/employee data breaches, 35% to financial loss, 33% to operational disruption, 36% to churn/loss of trust, and 24% to increased partner scrutiny.

Over a fifth (23%) see it as their biggest concern for the year ahead. And 60% claim such risks have become "innumerable and unmanageable". Open source software, booby trapped with malware or containing critical bugs, remains a particular concern. But so too are trusted proprietary software like MOVEit which can be targeted for mass data raids by zero-day exploits. And MSPs, which become a single source of failure.

Supply chains remain a critical feature of business operations – they also remain a fundamental weakness that threat actors are past masters at targeting.



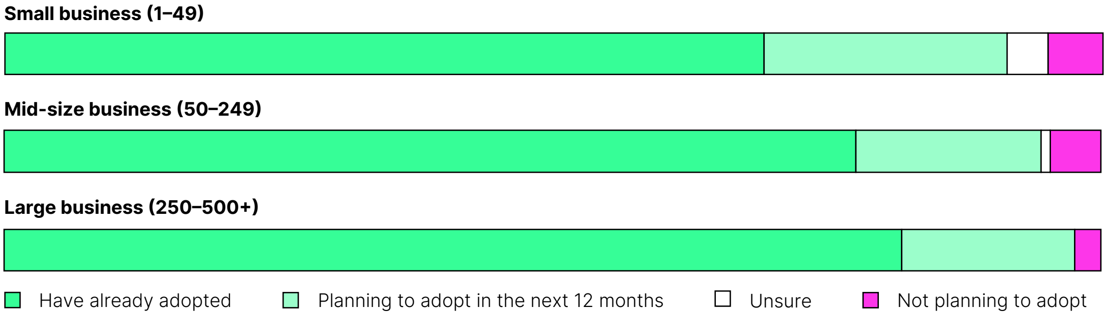
What were the impacts or repercussions of the third-party or vendor-related incident(s)?

A Force for Good

However, there are also signs that supply chains can have a positive impact on organisations, by forcing them to improve security. After all, 20% of respondents say that partner data has been compromised over the past year. For 29% of those organisations, the incident led to partner churn, while in 27% of cases it meant increased scrutiny from partners or suppliers. One of the biggest concerns responding organisations have about state-sponsored attacks is increased pressure from customers or partners, which are demanding enhanced resilience (34%).

That's part of the reason why 64% plan to increase spending on third-party risk management, and 80% have already done so over the past year. A fifth (21%) rank it a number one priority for the year ahead.

UK and US security leaders appear motivated to do better on infosec – not just because it will help prevent large-scale sup-



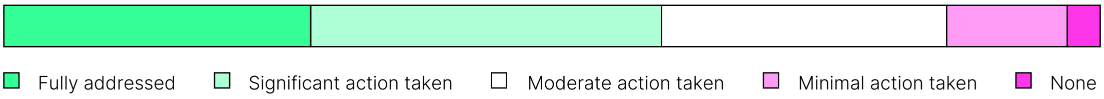
Have you, or are you planning to adopt initiatives to strengthen third-party and vendor risk management?

> ***The biggest threat arguably comes from the smallest suppliers. Only 71% claim to have strengthened vendor risk management (versus 82% of large businesses), and half plan to keep spending in this area at the same level next year or decrease it.***

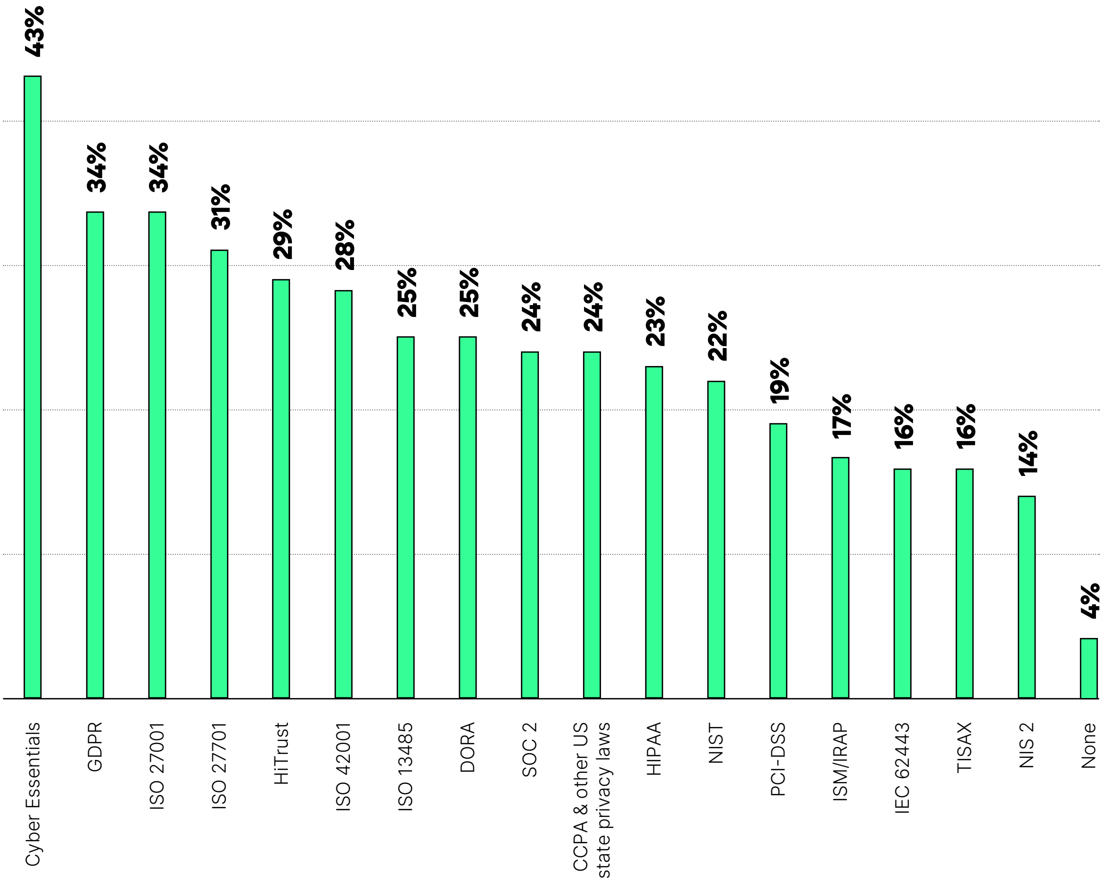
ply chain incidents (38%), but also because it will help their business enter new supply chains (23%). That's why 80% have strengthened third-party and vendor risk management over the past year, and 64% plan to increase spend on the area over the coming 12 months. Nearly all (96%) have reevaluated suppliers in line with geopolitical threats.

However, the biggest threat arguably comes from the smallest suppliers. Only 71% claim to have strengthened vendor risk management (versus 82% of large businesses), and half plan to keep spending in this area at the same level next year (45%) or decrease it (6%).

What action have you taken to address supply chain security and due diligence threats?



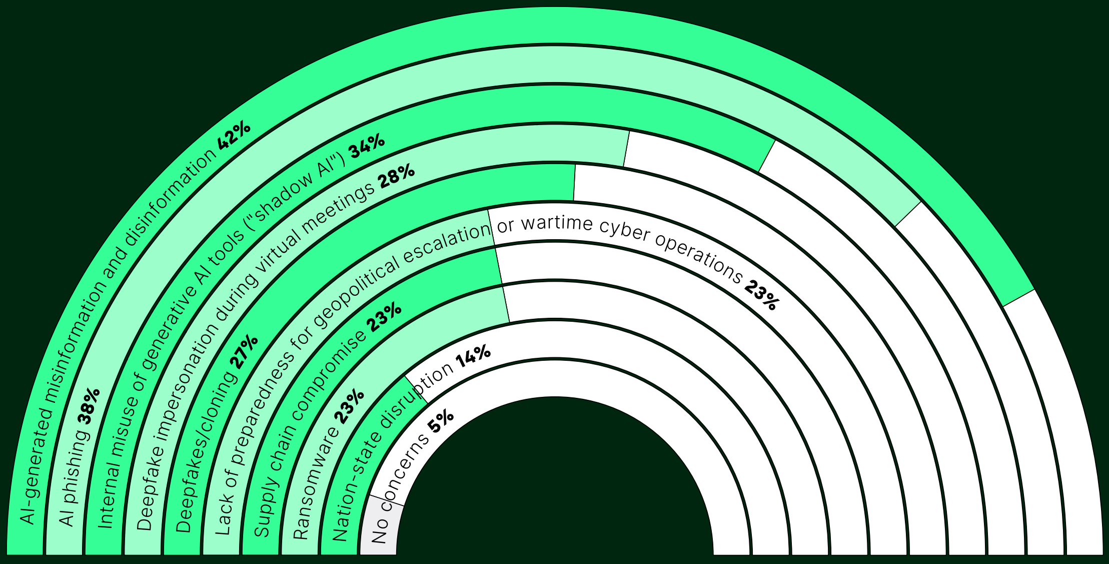
Which information security standards or regulations, if any, do you require of your suppliers to do business with them?



06

The world is a dangerous place

Geopolitical tensions are reshaping the threat landscape, with state-backed cyber operations and collateral risks extending far beyond government and critical infrastructure. For many organisations, resilience to geopolitical escalation is now a top security priority.



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

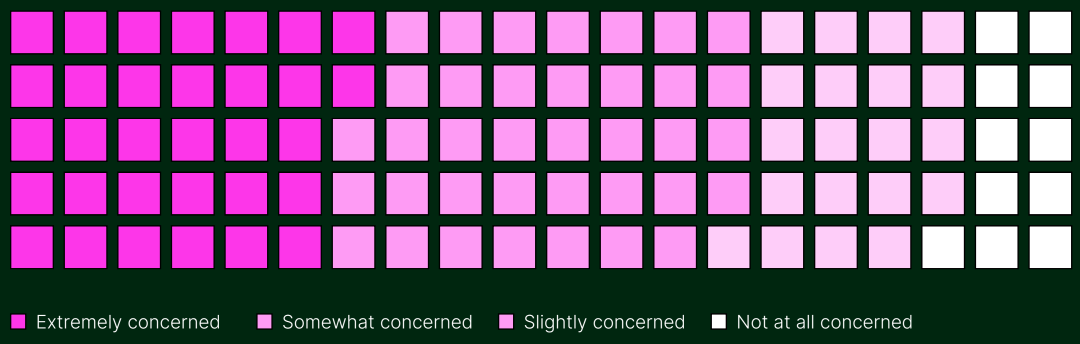
These are busy times for geopolitical risk analysts. As global power dynamics shift and the rules-based order established after the Second World War comes under strain, politicians and business leaders are right to be nervous. The World Economic Forum's Global Risk Report 2025 puts it clearer than most: state-based armed conflict is way out on top as the biggest perceived risk today. Yet a more uncertain world also has major implications in the cyber sphere.

Russia, Iran, and North Korea each pose distinct challenges. But perhaps none so much as China, whose cyber operations are on a scale and level of sophistication unmatched among the "RINCs" countries. Then there are the state-aligned hacktivists and the cybercrime groups allowed to flourish in former Soviet countries – both of which can cause problems.

> **_Nearly a quarter (23%) of respondents claim their biggest concern for the year ahead is a lack of preparedness for "geopolitical escalation or wartime cyber operations"._**

The risk is no longer only to government and critical infrastructure (CNI) providers. It is also to smaller suppliers (especially software developers) who may be attacked as a way to hit higher-value targets. And those who represent – purely by being a "Western" business – a legitimate target for financially motivated cybercrime or hacktivism. Many more may find themselves collateral damage, if they rely on goods or services produced by a targeted entity.

That explains why 88% of respondents fear state-sponsored attacks and nearly a quarter (23%) claim their biggest concern for the year ahead is a lack of preparedness for "geopolitical escalation or wartime cyber operations". And why a third (32%) claim that managing geopolitical risk is their primary motivation for strong infosec and compliance. Over a third (36%) also say they're concerned

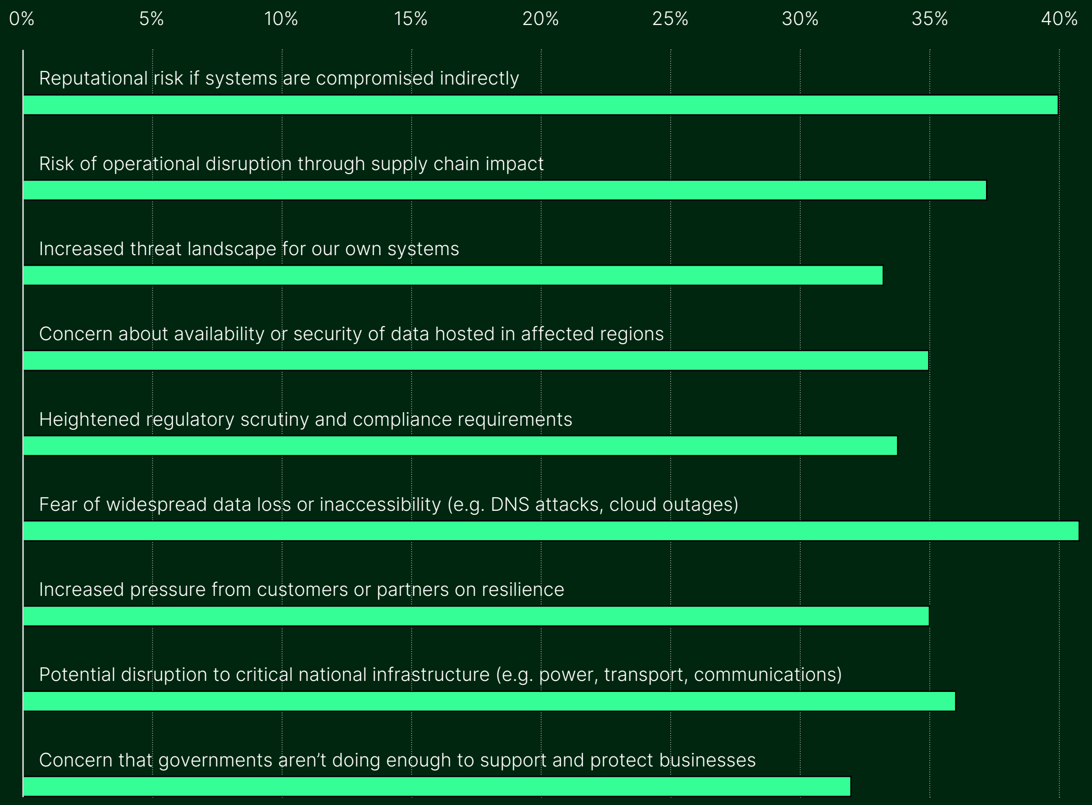


How concerned, if at all, are you about state-sponsored cyberattacks targeting your organisation?

about the impact of such threats on critical infrastructure, while 33% say governments aren't doing enough to support them. This may also explain why 74% claim already to have built resilience to such risks. And why doing so is a priority for a further fifth (19%) in the coming year.

Fully 88% say they're concerned about state-sponsored attacks specifically targeting their business. These could take many forms: from simple web defacement and DDoS to data theft and even destructive/ransomware-style attacks. That's why respondents' specific concerns range from data loss (41%) and reputational risk (40%) to supply chain-based operational disruption (38%) and CNI interruption (36%).

Smaller firms in particular could be at risk if singled out by nation states, given many have less to spend on security. Just 69% say they have adopted measures to strengthen resilience to these threats, some way behind their large-sized counterparts (76%). There's no indication of how comprehensive these measures were. However, it's heartening to see that the threat is at least understood, and steps are being taken to build resilience.



What concerns do you have about state-sponsored cyberattacks from a business perspective?

The Quantum Threat

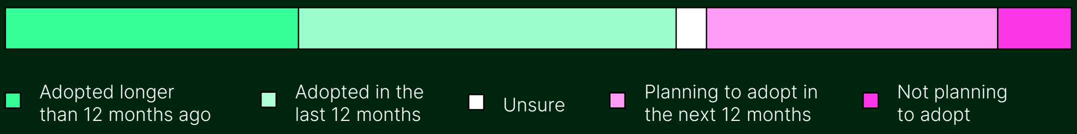
One longer-term risk that is fast approaching is of cryptographically relevant quantum computers (CRQCs). These are quantum computers capable of breaking the public-key cryptography on which most businesses rely to secure data and communications. Although such computers are several years away from reality, and even then, will only be viable for a small number of nation states, the threat is more urgent than it seems.

That's because of "harvest now decrypt later" (HNDL) attacks. This refers to the process of hackers stealing encrypted data today, with the view to decrypting it when CRQCs become available. Of course, this is only a risk for specific types of data, with a long shelf life, but it's still a threat. That's why it's heartening to see 63% of respondents have already adopted quantum-related security initiatives, and 61% are planning to increase spending on quantum computing security applications. A further 91% are planning to invest in "quantum risk readiness".

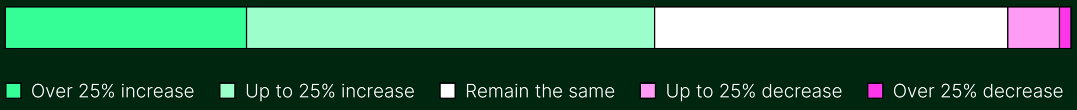
In practice, this work will require assessing what crypto they have in place, understanding their risk exposure to CRQCs, and developing a plan for migration to quantum-resistant cryptographic algorithms.

> ***One longer-term risk that is fast approaching is of cryptographically relevant quantum computers. Although such computers are several years away from reality, and even then will only be viable for a small number of nation states, the threat is more urgent than it seems.***

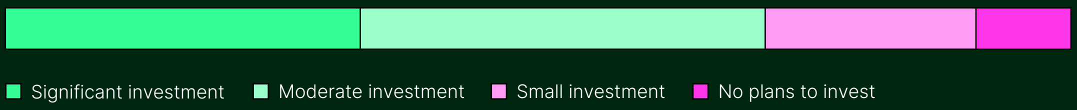
Have you, or are you planning to adopt quantum computing-related security initiatives in the next 12 months?



How do you expect your company's spend in quantum computing security applications to change in the next 12 months?



How much do you plan to invest in quantum risk readiness in the next 12 months?

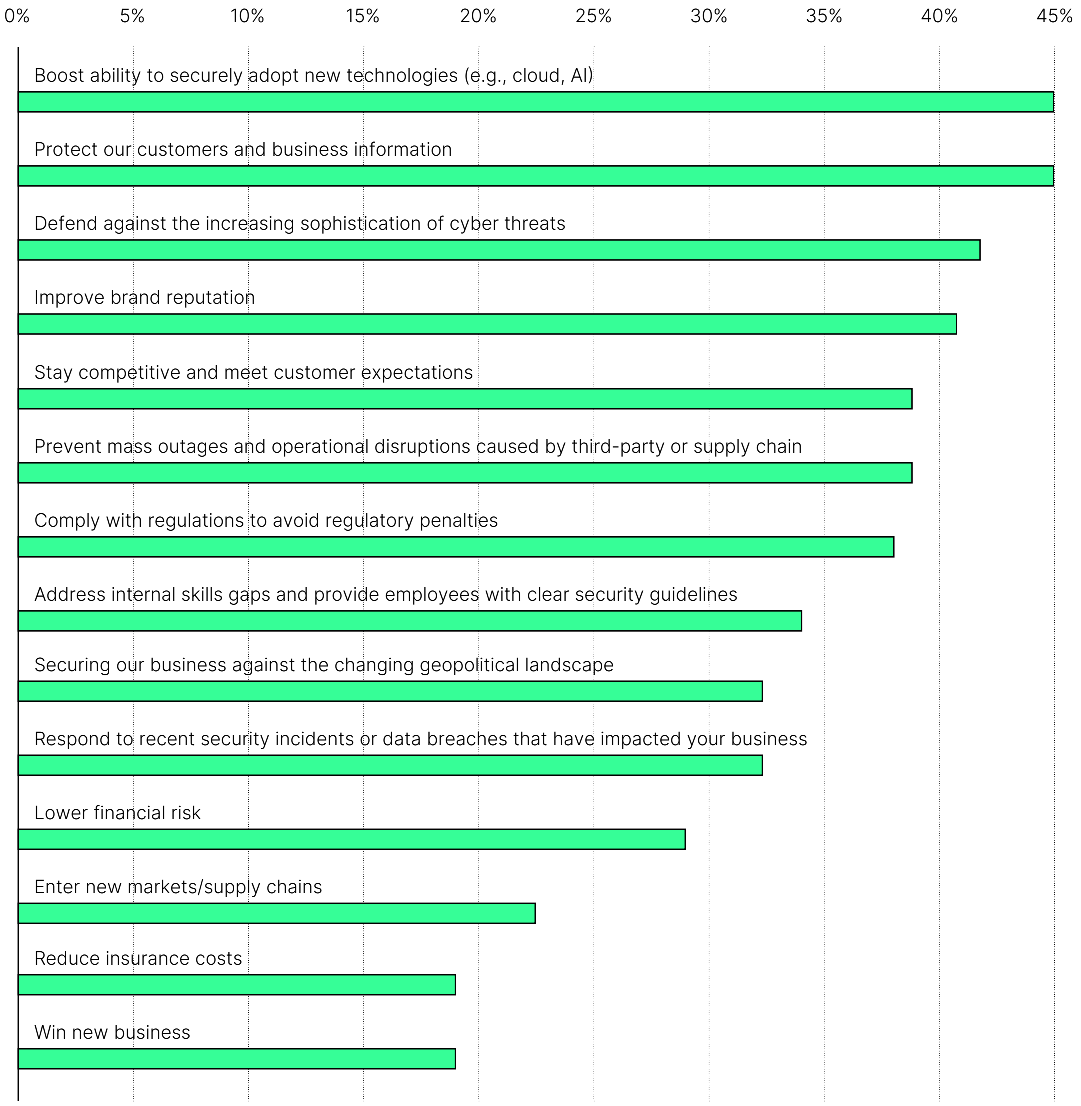


07

Securing tomorrow, building resilience

Despite a growing attack surface and evolving threats, organisations are increasingly treating information security as a driver of growth and trust. By prioritising resilience, they are preparing not just to prevent attacks, but to recover and thrive when they occur.

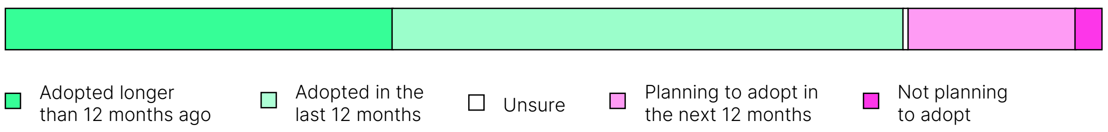
What, if anything, are your organisation's motivations for ensuring strong information security and compliance?



Although threats continue to evolve, attack surfaces expand and cyber risk worsens, our report is fundamentally optimistic about the future. That's because both American and British organisations appear to be switched on about the scale of the challenge and are taking proactive steps to address it.

This comes down to how cybersecurity is viewed and used in the organisation: not as an IT-focused function and cost centre but as an enabler which is critical to driving sustainable business growth. We can see this reflected in the motivations respondents have for ensuring strong information security and compliance. True, many define the mission in terms of avoiding risk – related to regulatory fines (37%), supply chain incidents (38%) sophisticated cyber threats (43%) and data breaches (32%). But many others cite drivers such as adoption of emerging tech (45%), protecting customers (45%), improving reputation (41%), and staying competitive (38%).

They also acknowledge that the best ROI they've got from compliance over the past year has been improved customer retention and trust (42%) better business decision making (44%) and enhanced reputation (38%).



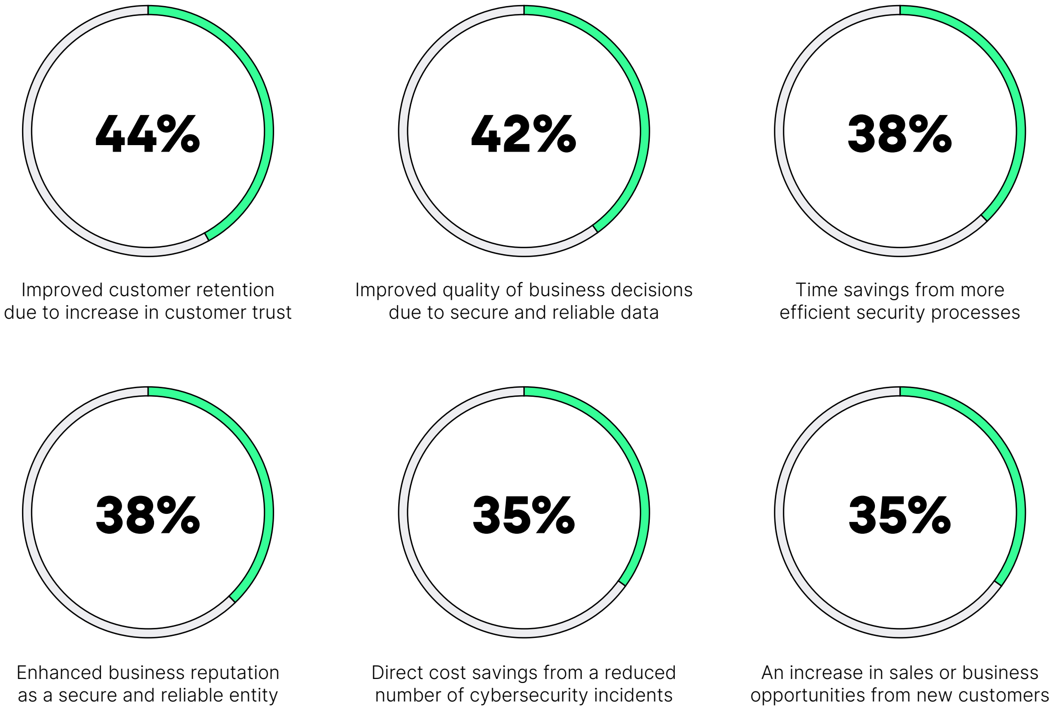
Have you adopted, or are you planning to adopt in the next 12 months strengthening of encryption standards and practices?

The journey to improved resilience

It follows from this business-focused approach to cybersecurity, that these organisations are investing in digital resilience. And they're doing so strategically rather than via reactive, one-off responses to breaches, which tend to result in money wasted on point solutions.

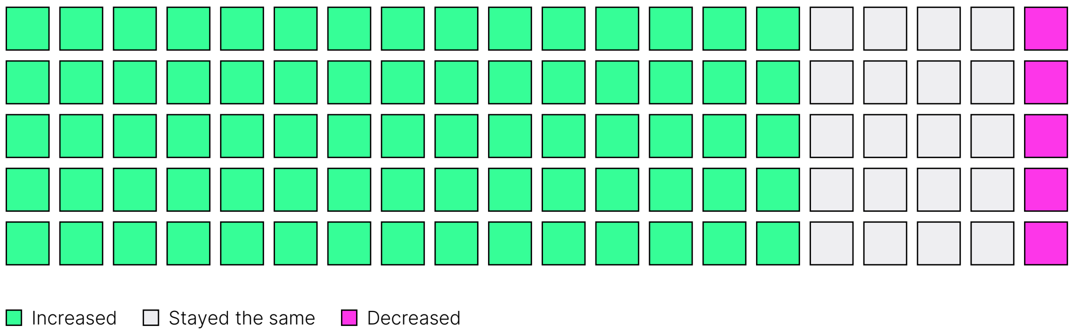
A great example is encryption – a fundamental best practice proven to help mitigate breach risk and accelerate compliance with PCI DSS and other standards/regulations. Some 83% of respondents say they have improved strengthening of encryption standards and practices. Although some sectors are still lagging (one in 10 legal businesses say they have no plans to do so), the overall trend is positive. The encryption story also extends to quantum readiness. Although it's several years out, the risk is being managed, with 91% planning to invest in it. Spending is projected to rise in all the areas IO quizzed responding organisations about, including cloud security (70%). This reflects an awareness of the growing cloud attack surface that has resulted from digital investments in this area, and the persistent probing of threat actors. Awareness extends to geopolitical risk and, most importantly, goes beyond awareness to action.

Arguably nothing will boost resilience more than effective incident response planning. Threat detection and response can help to reduce attacker dwell time, breach costs, damage and disruption – as well as surfacing insight to prevent similar attacks in the future. That's why we're heartened to see 97% of respondents having taken action in this area to address state-sponsored attacks.



Thinking about your information security compliance, what has provided the best ROI in the last 12 months? (top six responses)

Has your level of confidence in your cybersecurity changed in the past 12 months?



Preparing for the future

Respondents are not stopping there. They understand the skills, recovery and coordination issues highlighted by recent breaches and they're invested in improvements.

Over 86% feel confident in their ability to detect, defend against, and recover from AI-driven threats such as data poisoning, deepfakes, AI-powered malware, phishing and disinformation. But they're not taking this for granted – prioritising instead investments in enhancing defences against such threats (30%), and improving incident response (24%), digital authentication (24%) and employee awareness (24%).

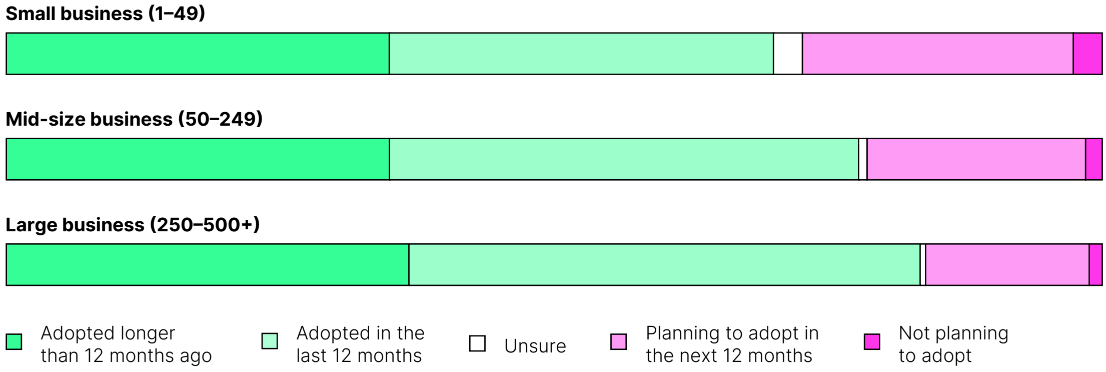
Additionally, 21% are focusing on responsible AI usage policies and 29% are planning to increase AI/ML security spend by over 25%. Some 95% are committed to improving AI governance, and a similar share is prioritising deepfake detection (94%) and GenAI-powered threat defence (96%).

Resilience is high on the agenda. Organisations know attacks will happen and their focus is on recovery and business continuity – to maintain trust with customers, regulators and other stakeholders.

Resilience is high on the agenda. Organisations know attacks will happen and their focus is on recovery and business continuity – to maintain trust with customers, regulators and other stakeholders.

One area of concern remains smaller organisations, which are less likely to invest in incident response (70% vs 82% of large businesses). That could be why only 46% say they're very confident in responding to a major security incident (vs 61% on average) and only 59% say their confidence in cybersecurity has increased over the past year (vs 75% on average). These businesses should prioritise testing incident response plans and improving recovery strategies – and be held accountable by their partners for doing so, given the supply chain implications.

Have you adopted, or are you planning to adopt, improving incident response preparedness and recovery capabilities?

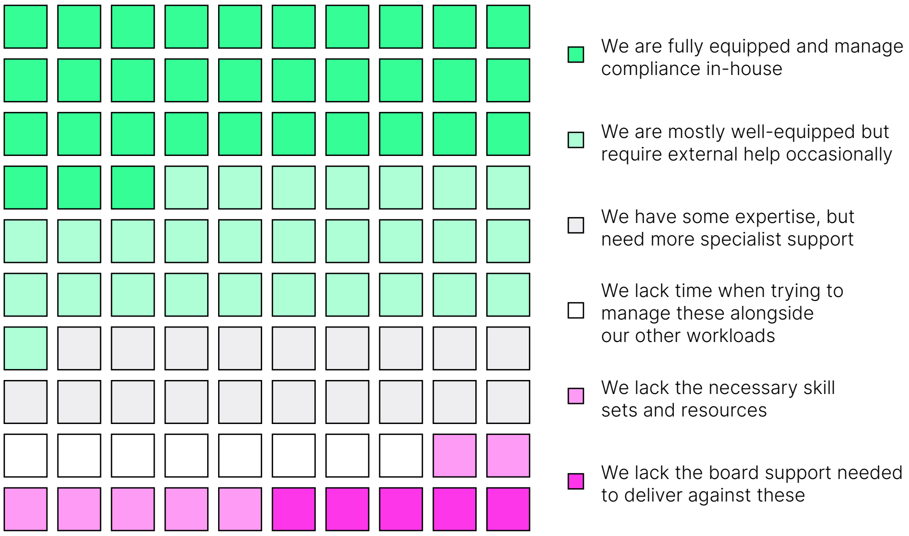


08

The compliance crunch

Compliance is no longer just about avoiding penalties. Organisations are recognising its role in driving trust, efficiency, and growth. Yet the speed and complexity of regulation mean many still struggle to keep pace, creating pressure that smaller firms feel most.

How well-equipped, if at all, do you feel your internal IT/ security team is to manage compliance with frameworks like GDPR, NIS2, and DORA?



Compliance is a journey rather than a destination. As we explained last year, an increasing number of businesses are seeing the benefits – not only in terms of avoiding risk but also laying the foundation for business growth.

While regulations are non-negotiable, best practice standards and frameworks are optional, so it's encouraging to see more respondents willingly adopt them. The likes of ISO 27001 and SOC2 offer a structured way to address cybersecurity in a risk-based way, with continuous improvement front and centre. The trend reflects a desire to transition from a reactive to a proactive, strategic security posture with resilience at its core.

No doubt driving these decisions is recognition of compliance ROIs such as customer retention (42%) improved quality of business decisions (44%), enhanced reputation (38%), and time savings from more efficient processes (38%). Respondents also cite an increase in new business opportunities (35%) and direct cost savings from a reduced number of incidents (34%). Interestingly, almost all of these business drivers are more frequently cited than mere avoidance of fines (35%).

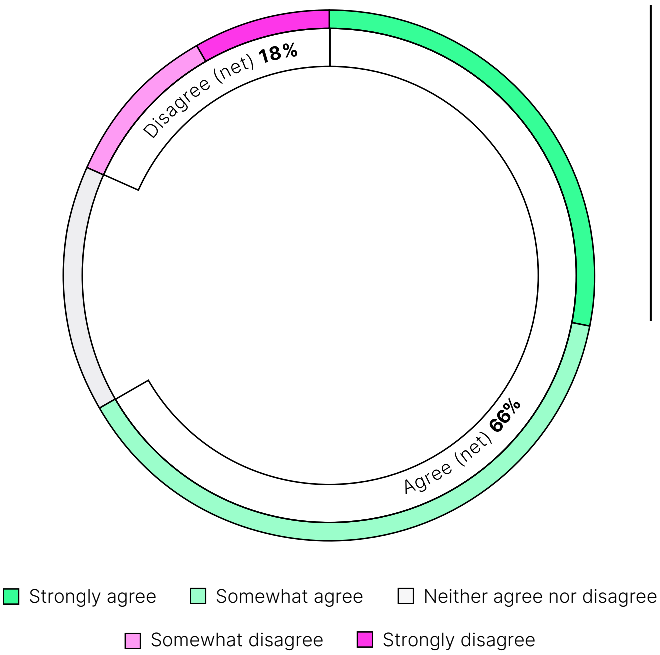
The positive news continues in that 87% of organisations say they clearly understand which regulations and frameworks their organisation needs to comply with.

Speed and complexity cause problems

However, not all organisations are progressing smoothly. Some 37% admit that compliance is a challenge, and two-thirds (66%) say that they're struggling to a lesser or greater extent to manage compliance in house. Half (48%) claim leadership still treats compliance as an afterthought. This is key. Like cybersecurity strategy in general, an effective compliance programme requires engaged leaders who understand the business value of compliance – as those ROI figures demonstrate.

Yet even with leadership on board, there are challenges. Many complain about the complexity of the regulatory landscape. Some 85% say more alignment on this front would

Despite these challenges, almost 96% of organisations list achieving or maintaining cybersecurity certifications as a priority.

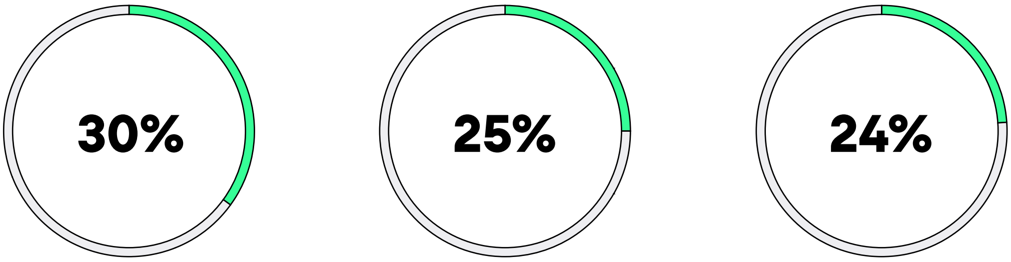


To what extent do you agree that the speed and volume of regulatory change make it increasingly difficult to stay compliant with information security standards

benefit their organisation, while two-thirds (66%) argue that the speed of regulatory change makes it difficult to stay compliant. Constant changes in regulations are the biggest bugbear of organisations complying with ISO 27001, NIS2, DORA, GDPR and CCPA. Costs and skills shortages are also frequently mentioned.

That could explain why a third (31%) of respondents say it takes 6-12 months to achieve ISO 27001 compliance, while a further fifth (20%) take over a year. A trusted compliance platform could help to accelerate these efforts. The need to improve compliance programmes is starkly illustrated by the share of respondents subject to regulatory scrutiny. Around a quarter experienced legal/regulatory costs and action following breaches of various data types in the past 12 months. Only 29% have not received a data protection fine in past 12 months. For nearly a third (30%) the fine was over £250,000. For some businesses, that will be an alarmingly high sum.

What many organisations are suffering, therefore, is a "compliance crunch". They feel they don't have the skills or resources to manage a complex, fast-moving regulatory landscape. The problem is particularly pronounced for smaller businesses – many of which still struggle with certification and compliance. Fewer are aligned with



Enhancing defences against AI-generated threats

Achieving or maintaining cybersecurity certifications (e.g. ISO 27001, SOC 2)

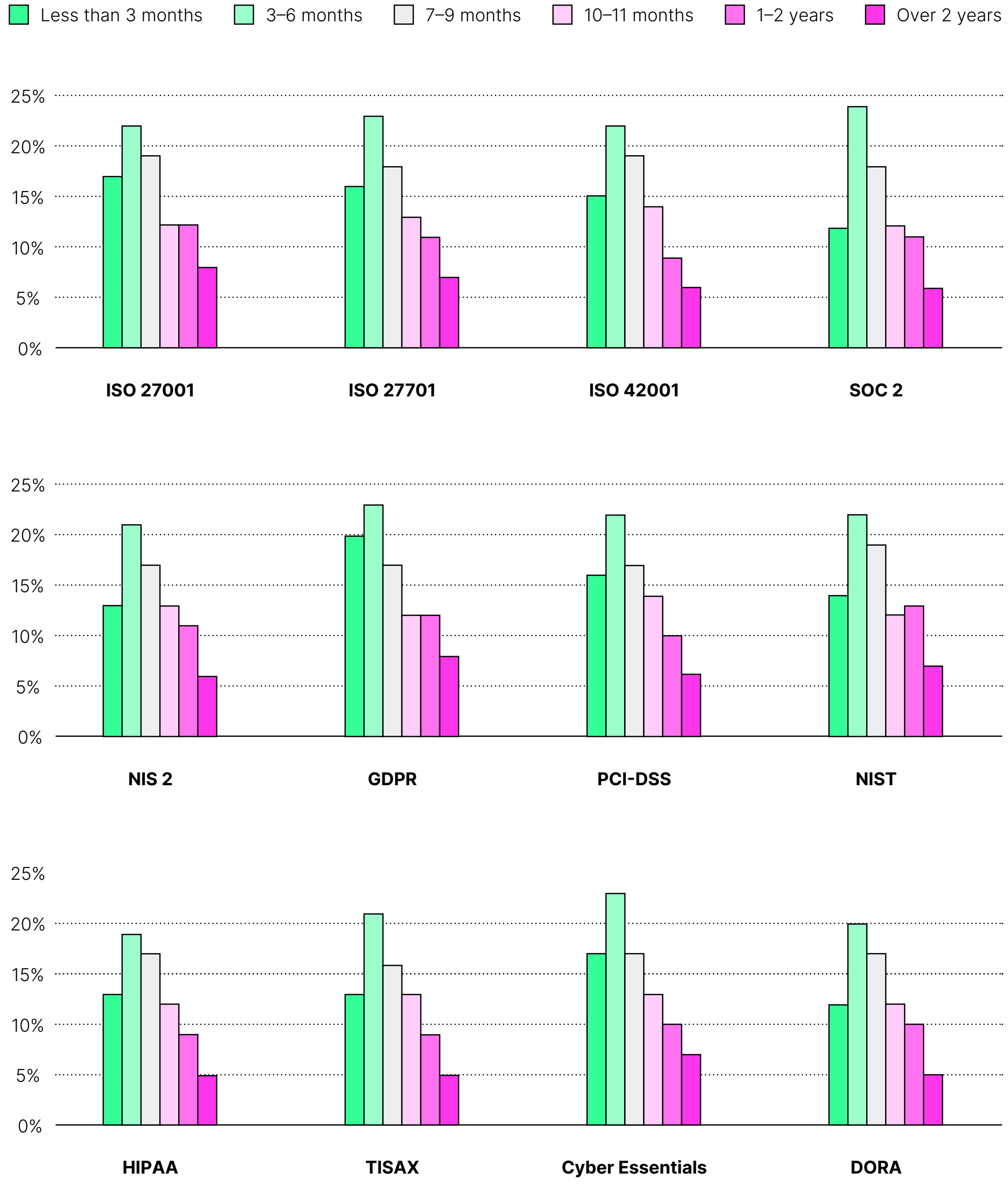
Improving incident response preparedness and recovery capabilities

What are your organisation's top information security priorities for the next 12 months?

information security regulations, standards and certifications like ISO, and only 29% feel fully equipped to handle compliance in-house. This “compliance crunch” is widening the gap between those able to turn compliance into a competitive advantage and those left exposed to risk, lost opportunities, and mounting regulatory pressure.

Despite these challenges, almost 96% of organisations list achieving or maintaining cybersecurity certifications as a priority, recognising that these offer a great way to minimise the regulatory burden. This reflects a growing understanding that robust compliance is the foundation for responsible, successful business.

How long did it take to achieve compliance with the following frameworks and regulations?

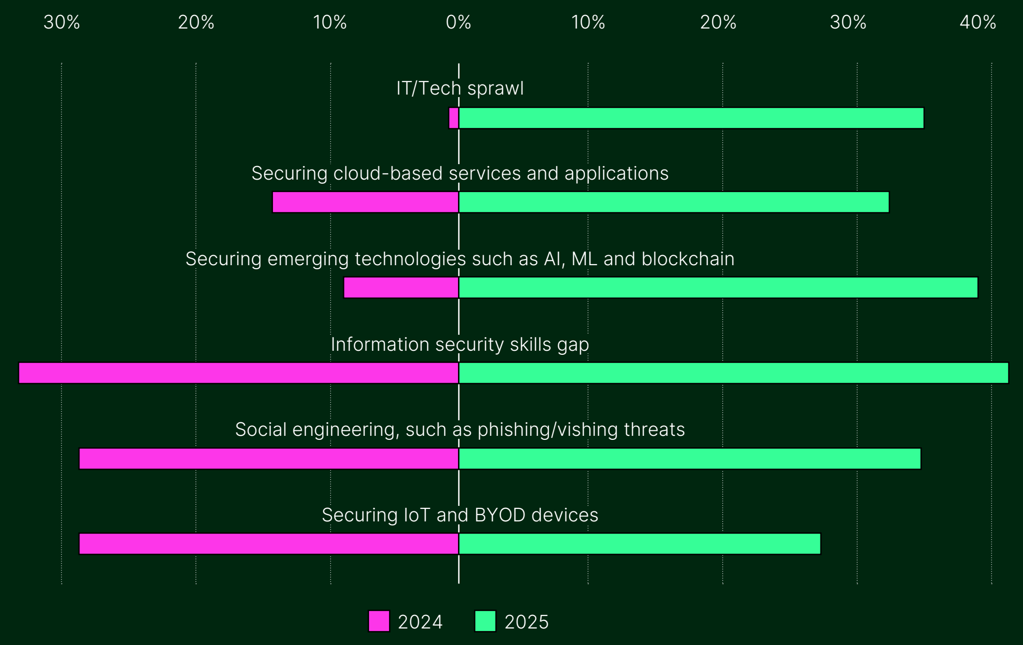


09

How times have changed

Information security priorities are shifting fast as organisations confront tech sprawl, cloud risks, and regulatory complexity. Encouragingly, more are moving beyond reactive measures, adopting clearer strategies and stronger supplier standards to build resilience.

Year-on-year comparison for types of challenges you are currently facing in information security 2024 vs 2025



Cybersecurity doesn't exist in a vacuum. Strategy changes as infrastructure evolves and the threat landscape continues to develop. That's why it's interesting to see exactly how organisations in the US and UK are responding to different challenges. The good news is that, for the most part, spending and supplier scrutiny are increasing, and strategic thinking, rather than reactive chaos, is the direction of travel.

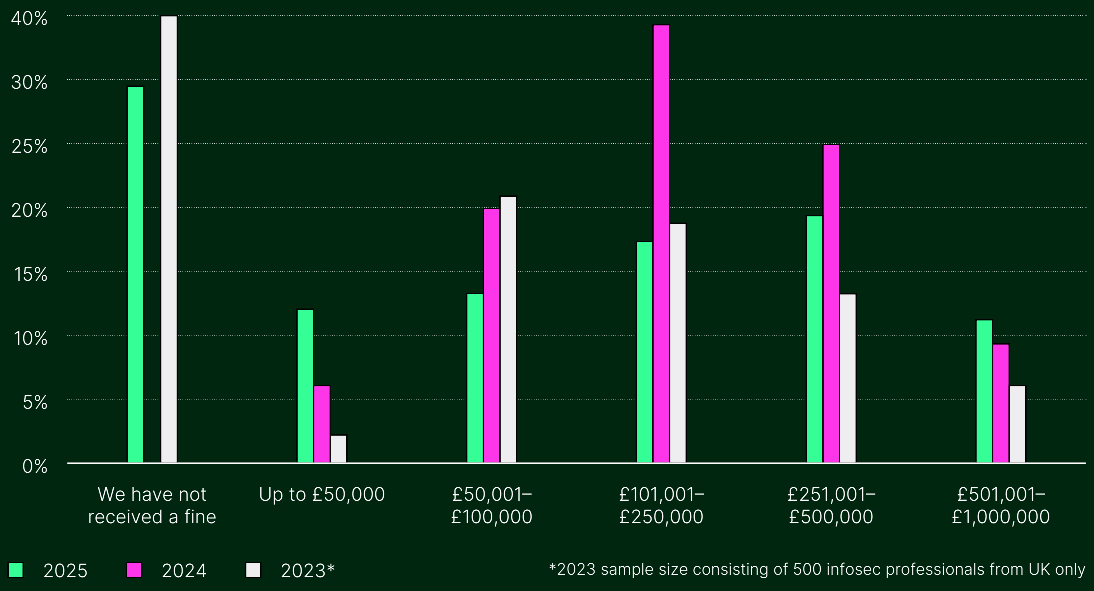
Challenges and incidents

Among the biggest leaps in current challenges is tech sprawl, which was cited by just 1% in 2024 but is now an issue for over a third (35%) of respondents. As organisations continue to invest in digital infrastructure, their attack surface expands, and visibility and control gaps emerge. In a similar vein, securing cloud services and apps (14% to 33%) and securing emerging tech like AI (9% to 39%) saw big increases. The share of respondents citing challenges with skills gaps (33% to 42%), and social engineering (29% to 35%) increased slightly.

Big surges can also be observed in terms of certain types of incidents experienced over the previous 12 months. Phishing (12% to 30%), cloud breaches (10% to 27%), supply chain compromise (7% to 15%) and IoT/mobile breaches (10% to 19%) were among the most notable. Authentication breaches surged tenfold, from 2% to 20%, highlighting the growing security threat posed by compromised credentials. There were more modest increases for data breaches (21% to 31%) and network intrusions (16% to 24%).

Interestingly, the share of respondents reporting malware, deepfakes, insider threats, ransomware and DDoS all declined. In the case of deepfakes, the drop was 13%, although as discussed, other AI threats have surged at the same time. The share of companies reporting third-party incidents declined from 81% to 61% over the year.

The good news is that, for the most part, spending and supplier scrutiny are increasing, and strategic thinking, rather than reactive chaos, is the direction of travel.



*2023 sample size consisting of 500 infosec professionals from UK only

What is the total amount your business has received in fines for a data breach or violation of data protection rules in the last 12 months?

Compliance

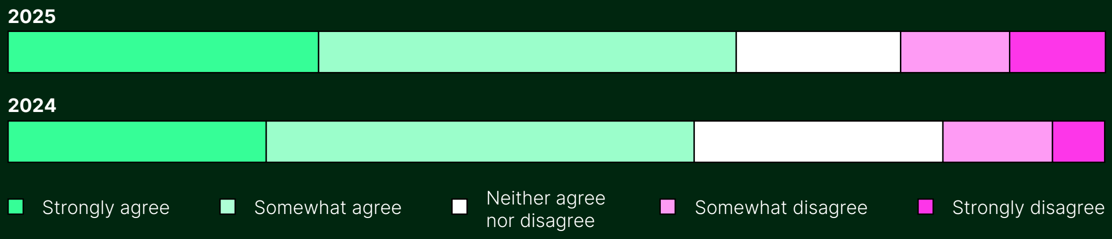
As we've discussed, organisations are finding it increasingly difficult to keep pace with the regulatory landscape. The share who said the speed and volume of change makes compliance difficult rose from 61% in 2024 to 66% this year. Those calling for more regulatory alignment across jurisdictions surged even further – from 63% to 85%.

For many, the motivation for security and compliance is changing too. We saw the biggest increases in the share of respondents citing secure adoption of new technologies (12% to 45%), defence against sophisticated threats (6% to 43%), improved brand reputation (16% to 41%) and avoiding regulatory penalties (18% to 37%).

The latter is interesting, given that we also saw a heartening increase (from 0% to 29%) in the share of organisations reporting no fines over the past 12 months. Only for fines of £0-£50,000 (6% to 12%) and £501,001-£1,000,000 (9% to 11%) did the figures tick up.

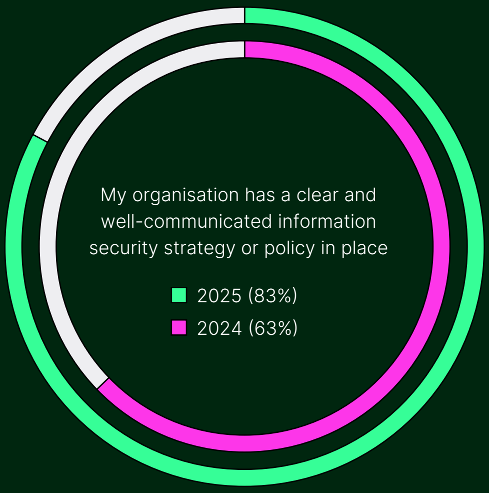
Responding organisations are also placing greater scrutiny on their suppliers, which has to be a good thing. Those who now require Cyber Essentials shot up from 8% to 43%. That may be because it is arguably the easiest certification to obtain. Another big increase was for ISO 42001 (1% to 28%), which governs secure AI. That fits the narrative of digital transformation. Elsewhere we also saw the share of respondents citing SOC2 (13% to 24%) almost double, while NIST CSF (9% to 22%) increased in popularity, and GDPR (9% to 34%) surged even further.

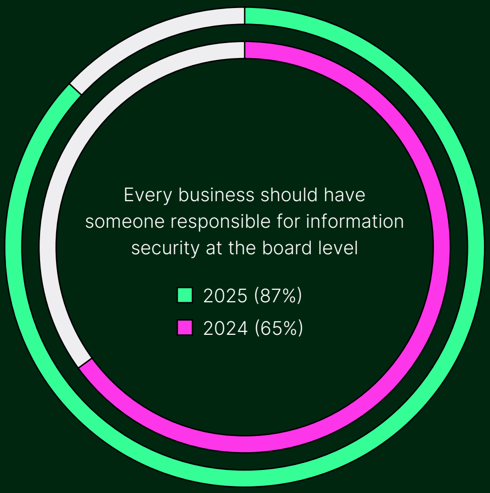
US state privacy laws are also starting to kick in, with the figure requiring this of suppliers increasing from 11% to 24%. There were also more modest increases for ISO 27001 and ISO 27701.



The speed and volume of regulatory change make it increasingly difficult to stay compliant with information security standards

How times have changed





Strategic planning

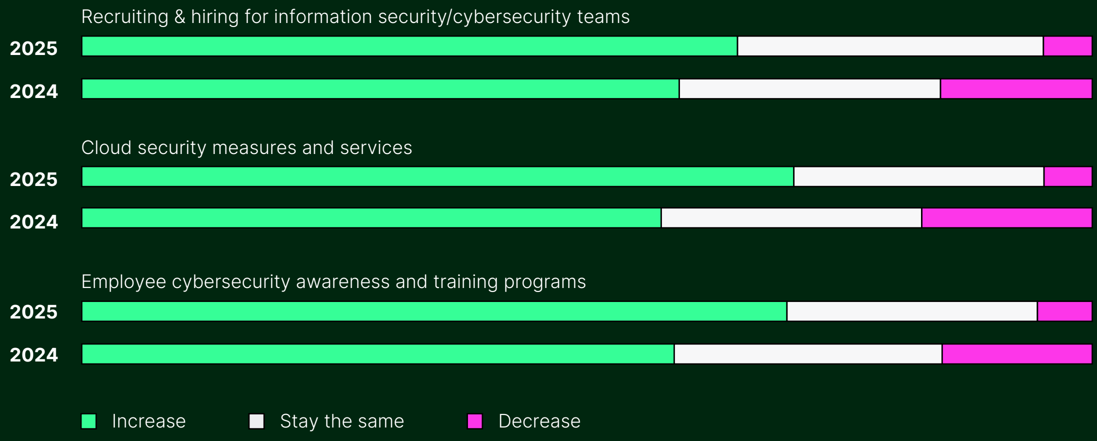
Above all, respondents are becoming more strategic. Literally. Those claiming to have a clear and well-communicated information security strategy in place increased from 63% last year to 83% this. Also telling is the share agreeing that every business should have someone responsible for information security at the board level. This rose from 65% to 87%.

Fuelling this evolution in how cyber risk and compliance is viewed and managed could be the concrete ROI that many respondents are seeing from their efforts. There were big increases in those reporting an improvement in business decisions (26% to 44%), customer retention (16% to 42%), and sales opportunities (13% to 35%) – all positive strategic drivers of security and compliance. Of course, there were also increases in more tactical drivers like lowering insurance premiums (11% to 27%) and reduced IP theft (6% to 28%).

As for the future, it's heartening to see so many more organisations in the US and UK pledging to increase spend on hiring security staff (59% to 64%), cloud security (58% to 70%), security awareness training (59% to 69%), encryption (60% to 67%), network security (53% to 67%) and compliance (57% to 63%).

Above all, respondents are becoming more strategic. Literally. Those claiming to have a clear and well-communicated information security strategy in place increased from 63% last year to 83% this.

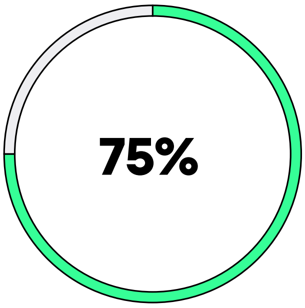
How do you expect your company's information security spend to change in the next 12 months, in the following areas?



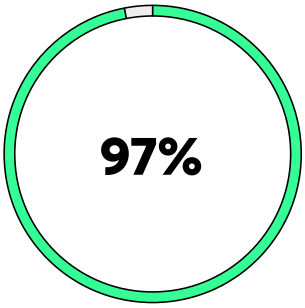
10

Conclusion

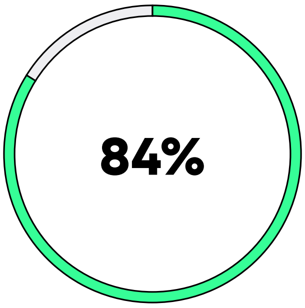
Organisations face rising AI-powered and state-sponsored threats, yet confidence is growing. A shift toward strategy, resilience, and long-term planning marks a new phase in information security, one that must extend to smaller firms to raise the baseline.



Say their confidence in cybersecurity has increased over the past year



Are confident about their ability to respond to a major incident



Feel prepared to handle the next generation of AI-powered threats

British and American organisations of all sizes are preparing for a new wave of AI-powered threats and elevated risk stemming from their expanding attack surface. They must do so while addressing the less headline-grabbing but persistent threats to the rest of their infrastructure. Most (88%) are also concerned about the growing risk of state-sponsored attacks, and the financial, reputational and compliance impact of breaches.

Yet an overwhelming majority (75%) say their confidence in cybersecurity has increased over the past year, and even more (97%) are confident about their ability to respond to a major incident. Over 84% feel prepared to handle the next generation of AI-powered threats. This speaks to a subtle evolution in thinking on cybersecurity: one driven from the top down.

We're seeing growing investment in incident response and other resilience measures that speaks to the emphasis organisations now place on strategic planning over reactive firefighting. Their plans to invest in quantum risk readiness are typical of this new way of thinking. But it doesn't end here. The mindset is shifting from patching problems piecemeal today to long-term resilience for tomorrow.

Some 86% of responding organisations now claim to have a clear and well-communicated information security strategy or policy in place. The challenge for the coming year, will be to increase that figure, especially among smaller organisations. Making it easier for them to adopt best practice standards, certifications and frameworks could be the key to getting there.

We're seeing growing investment in incident response and other resilience measures that speaks to the emphasis organisations now place on strategic planning over reactive firefighting. The mindset is shifting from patching problems piecemeal today to long-term resilience for tomorrow.

In focus

Compliance is no longer just about avoiding fines, it's becoming a driver of trust, resilience, and growth. Here, our CPO shares why consistency and confidence are now central to every security strategy.

Sam Peters

Chief Product Officer

io

As regulations continue to evolve, strong compliance won't just protect against penalties; it will become one of the main drivers of trust and long-term resilience.

This year's research makes one thing clear: compliance is now central to security strategy. Seventy-one per cent of organisations received fines in the past 12 months, and nearly a third of those penalties were more than £250,000. Two-thirds of respondents told us they struggle to manage compliance in-house, pointing to the speed of regulatory change and the lack of alignment across jurisdictions. These aren't small challenges; they're fundamental to how secure and resilient a business can be.

What's encouraging is how the conversation around compliance is shifting. It's not just about avoiding penalties anymore. Many organisations are using standards like ISO 27001 and SOC 2 to build customer trust, strengthen decision-making, and even open new business opportunities. Done well, compliance does more than reduce risk; it supports growth.

Done well, compliance does more than reduce risk; it supports growth.

The difficulty, of course, is consistency. With regulations moving quickly and frameworks overlapping, manual or fragmented approaches don't hold up for long. That's why more leaders are looking for platform-based solutions, ways to consolidate compliance under one roof, cut duplication, and provide the confidence that nothing critical is being overlooked.

That idea of compliance confidence is becoming essential. It's about being able to show customers, partners, and regulators that the organisation is prepared, without exhausting already stretched teams. And as regulations continue to evolve, strong compliance won't just protect against penalties; it will become one of the main drivers of trust and long-term resilience.

Explore more at **isms.online**