Public V1.0

United States Edition 

The state of information security report 2025

The state of information security report 2025

United States Edition 

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 US 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

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.

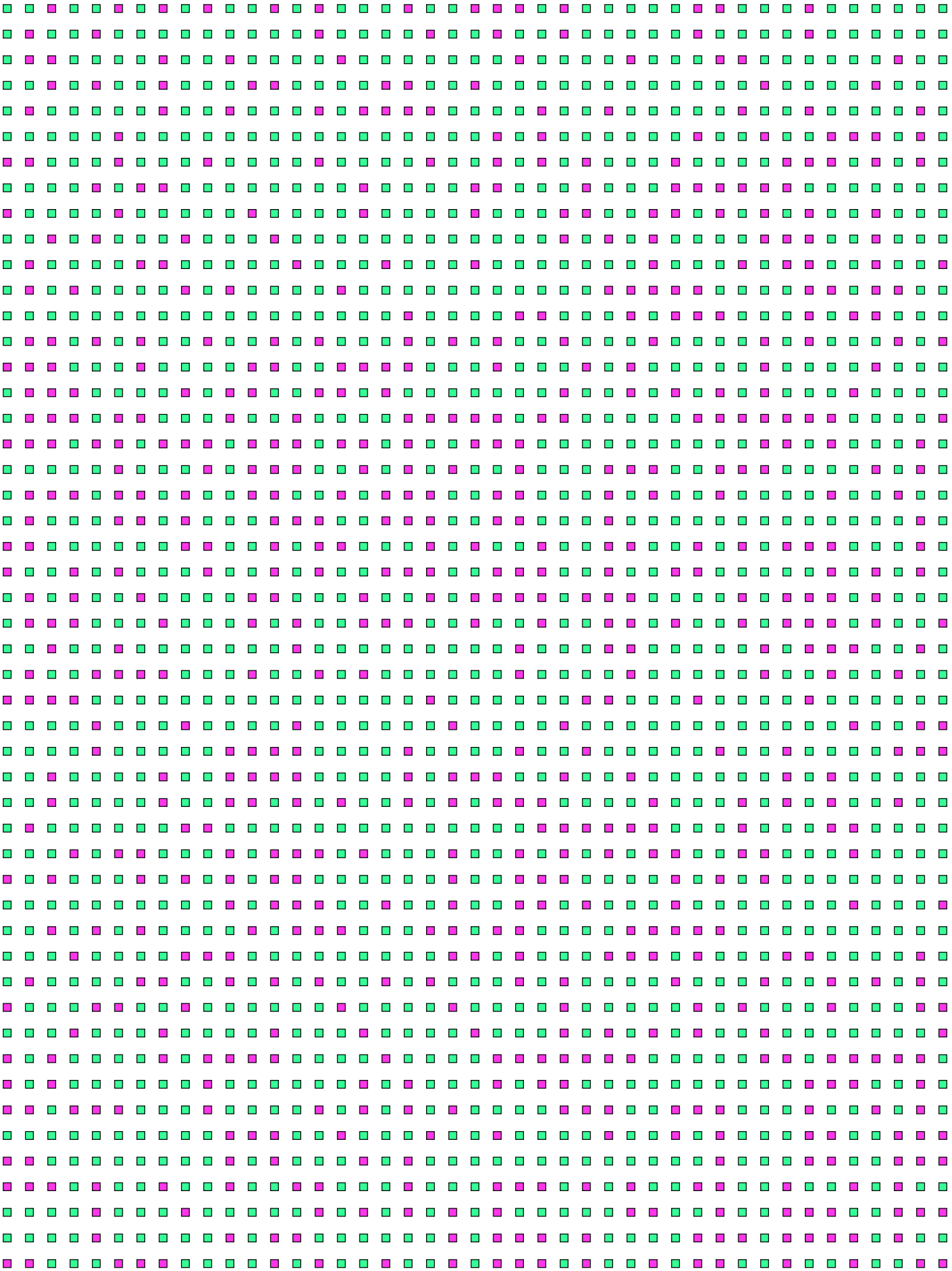
US organisations have leaned into digital change over the past year. From rolling out cloud services, experimenting with AI, and adopting new tools, staying ahead is the name of the game. But with each of these changes comes added exposure. The attack surface keeps expanding, and attackers are quick to take advantage.

Our US State of Information Security Report 2025 shows just how complicated the attack landscape has become for organisations. 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. While AI is proving to be a powerful asset, it also represents a new source of risk, with shadow AI and data poisoning high on the list of emerging concerns.

The financial impact is also notable. Three in four US organisations received fines for a data breach or violation of data protection rules in the past year; over a third (35%) of those penalties were more than $330,000. As a result, there's been a striking shift in how businesses view compliance. Firms that perhaps previously viewed compliance as simply a barrier to innovation and a way to avoid fines are using frameworks such as ISO 27001 and SOC 2 to strengthen trust, sharpen decision-making, and even enable 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.



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).

This snapshot report is based on the answers provided by our 1,001 US respondents. 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)

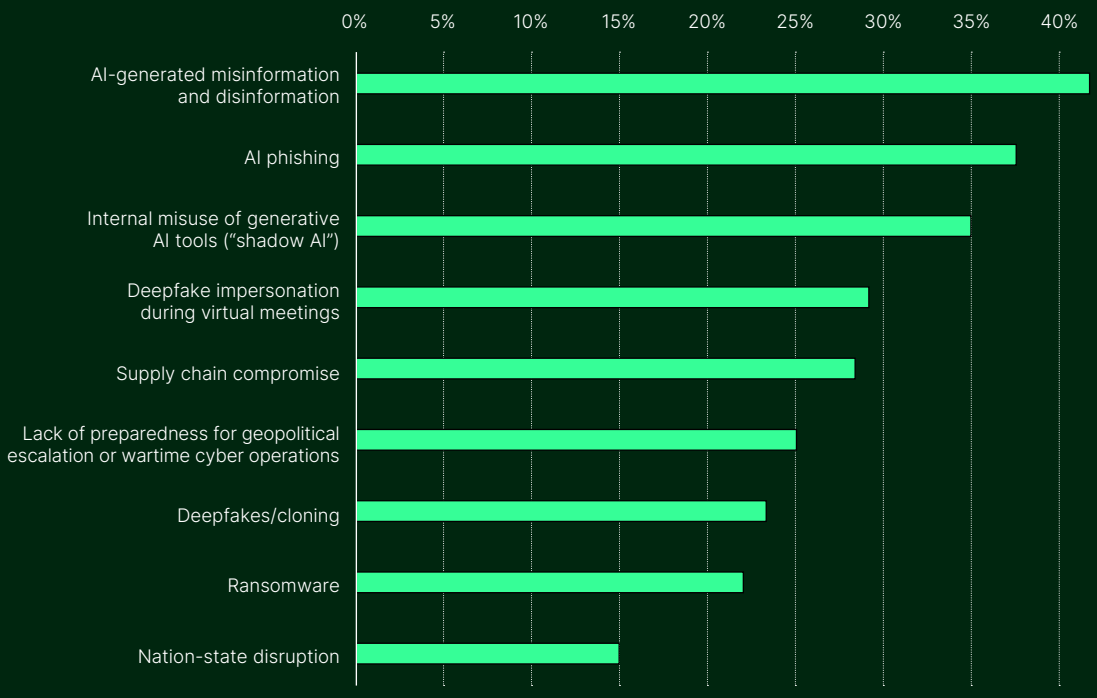
US respondents (1,001)

Introduction

If there's one thing this year's US State of Information Security Report highlights, it's the myriad ways in which artificial intelligence (AI) is changing the cybersecurity landscape.

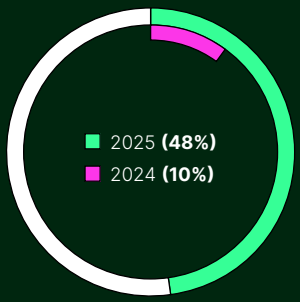
US respondents indicate that AI-driven attacks represent the biggest emerging threat to their businesses. More than two in five (43%) say they're concerned about AI-generated misinformation and disinformation (43%), followed by AI phishing (39%). One in three (36%) are concerned about shadow AI, where employees use Generative AI (GenAI) outside organisational controls.

This new threat landscape has triggered notable changes in organisations' motivations for ensuring information security and compliance. Over two in five (43%)

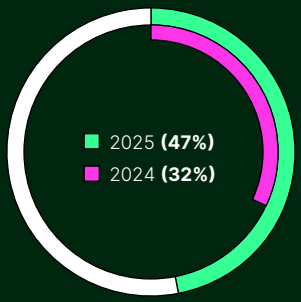


What, if anything, are your biggest emerging threat concerns for the next 12 months?

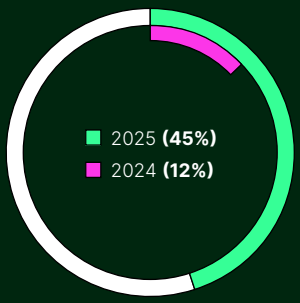
What, if anything, are your organisation's motivations for ensuring strong information security and compliance?



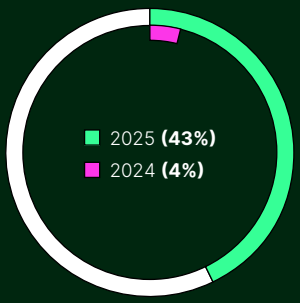
Boost ability to securely adopt new technologies (e.g., cloud, AI)



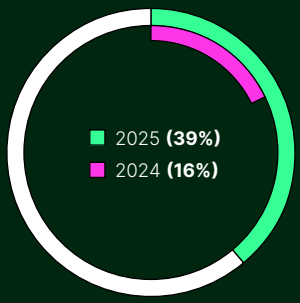
Protect our customers and business information



Improve brand reputation



Defend against the increasing sophistication of cyber threats



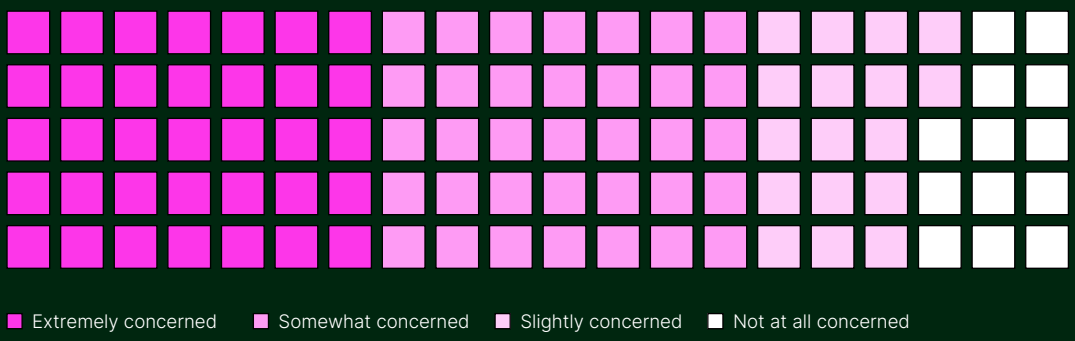
Comply with regulations to avoid regulatory penalties

respondents cite defending against the increasing sophistication of cyber threats as one of their organisation's motivations, compared to just 4% of respondents in 2024. Nearly half (48%) say that boosting their ability to securely adopt new technologies like cloud and AI is a motivator, another considerable jump from 10% in last year's report.

80% of US organisations have adopted new technologies like AI, ML and blockchain for security already, and 18% say they plan to do so in the next 12 months. Despite the growing attack surface AI presents for threat actors, business leaders also see the potential for AI as a catalyst of security, innovation, and growth.

Emerging risks like geopolitical threats – 87% of organisations are concerned about state-sponsored cyberattacks – are adding to the chaos. Meanwhile, quantum computing capabilities are inching closer to becoming reality. The last twelve months have been a busy time for CISOs and their teams, and the year ahead looks set to be equally intense.

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

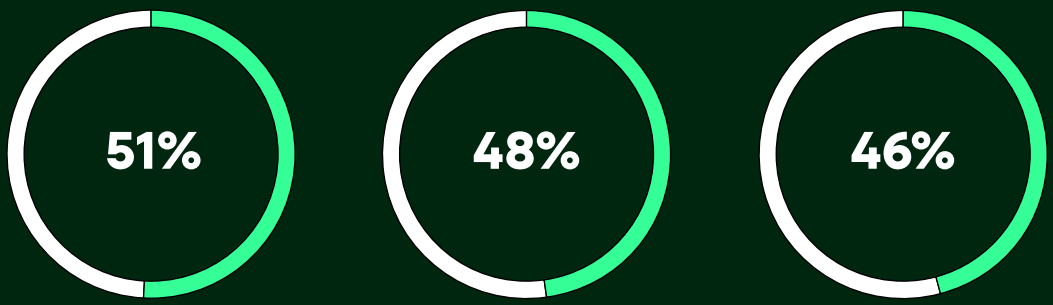


Top cybersecurity challenges

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.

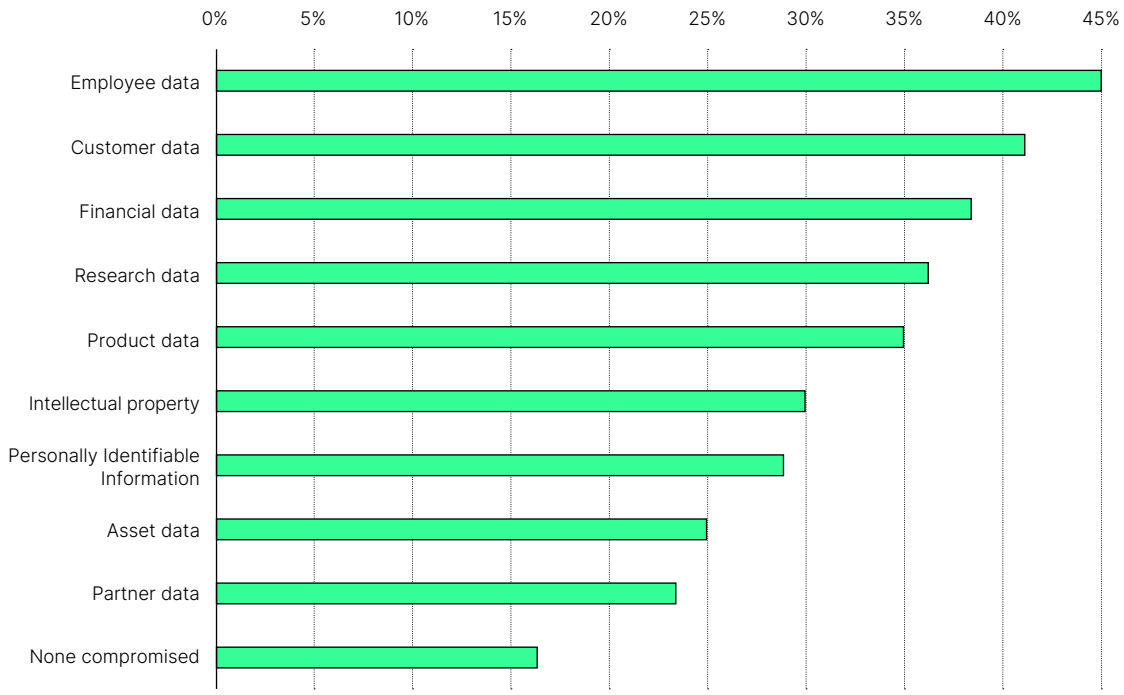
For US organisations, the biggest cybersecurity and information security challenges remain the same, but they're impacting more businesses than ever. Over half of respondents (51%) say the information security skills gap is their biggest challenge, compared to a third (33%) last year. There are simply not enough information security professionals to meet demand for their skillset.

The top three challenges are rounded out by ensuring third-party risk is managed and tracking compliance (48%) and IT/tech sprawl (47%). Perhaps unsurprisingly, given the evolving threat landscape, digital resilience (46%) and securing emerging technologies like AI, ML and blockchain (45%) are also top issues for organisations.



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

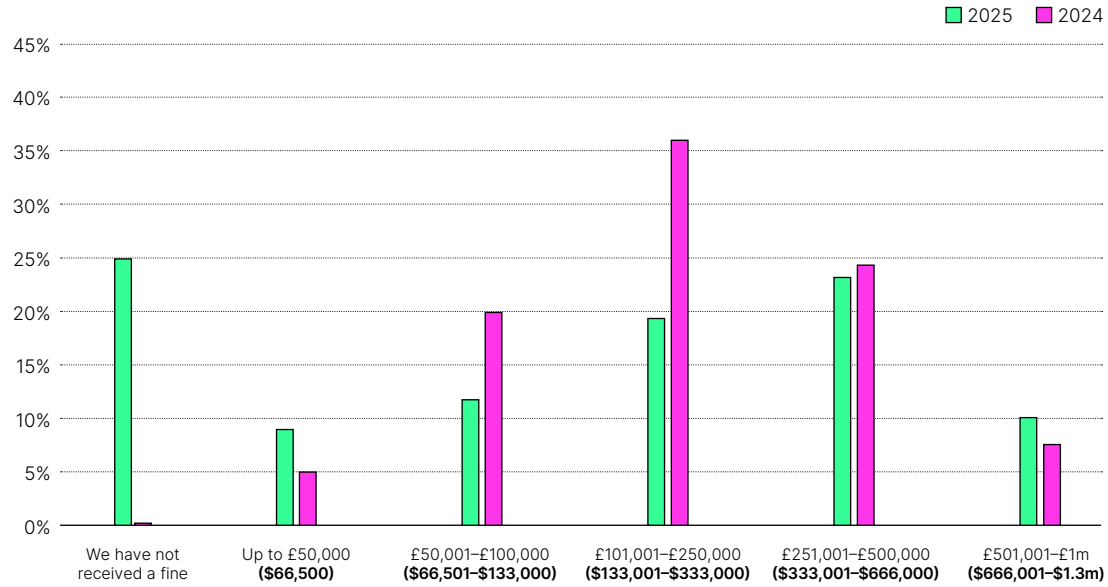
Which types of data have been compromised in your organisation in the past 12 months?



US respondents saw significantly higher levels of data compromise than last year. Nearly half (45%) of US businesses saw employee data compromised, compared to 13% in last year's report. Two in five (41%) say customer data was compromised, up from 29% last year, However, financial data compromise has decreased slightly, from 42% last year to 39% this year. With these figures in mind, it's perhaps no surprise that over a third (34%) of US organisations received fines of £250,000 ($333,000) or more for data breaches or violation of data protection rules.

Notably, these data compromise figures are considerably higher than those reported by UK respondents. They reflect the ways in which organisations are grappling to resolve issues caused by sophisticated cyber threats, like AI-powered attacks, and ensure compliance with regulations and industry standards, which 39% say remains a challenge.

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?



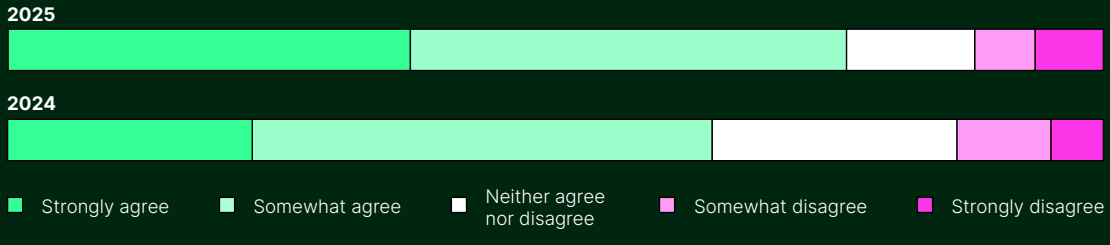
The compliance opportunity

Many organisations struggle to address disparate global compliance requirements, but there's no doubt US respondents see the value in their information security compliance.

Nearly three quarters (74%) of respondents say the speed and volume of regulatory change make it difficult to stay compliant with information security standards and 88% say greater global collaboration and regulatory alignment on information security would benefit their organisation. However, nearly all (96%) have achieved or plan to invest in cybersecurity certifications like ISO 27001 and SOC 2, helping them to drive trust and growth.

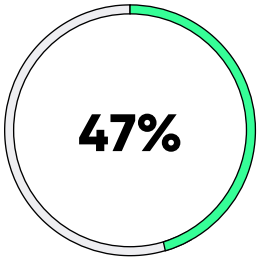
Report data supports these goals: nearly half (47%) say the best compliance-related ROI has been improved customer retention due to increased trust, while 35% say the best ROI comes from avoiding compliance-related fines and penalties. Both outcomes support an organisation's bottom line as well as building opportunities for future growth.

Organisations are increasingly proactive when it comes to compliance, too. 74% say they have prepared for upcoming regulatory changes and new compliance obligations, while 22% are planning to do so in the next 12 months. The majority (88%) also clearly understand with which regulations and frameworks their organisation needs to comply.

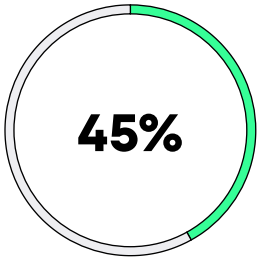


The speed and volume of regulatory change make it increasingly difficult to stay compliant with information security standards

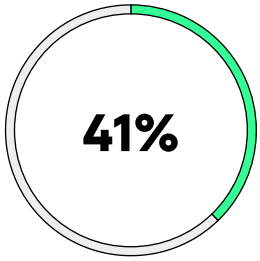
Thinking about your information security compliance, what has provided the best ROI in the last 12 months? (top six responses)



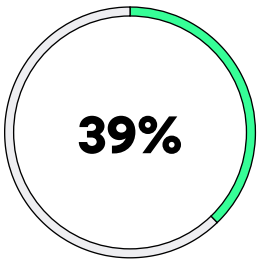
Improved customer retention due to increase in customer trust



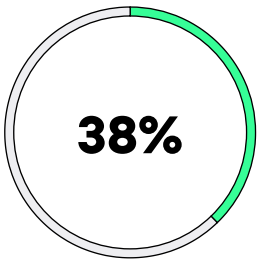
Improved quality of business decisions due to secure and reliable data



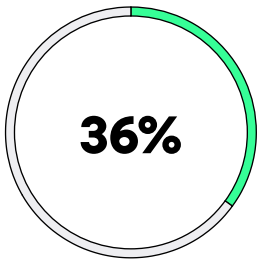
Time savings from more efficient security processes



Enhanced business reputation as a secure and reliable entity



Direct cost savings from a reduced number of cybersecurity incidents

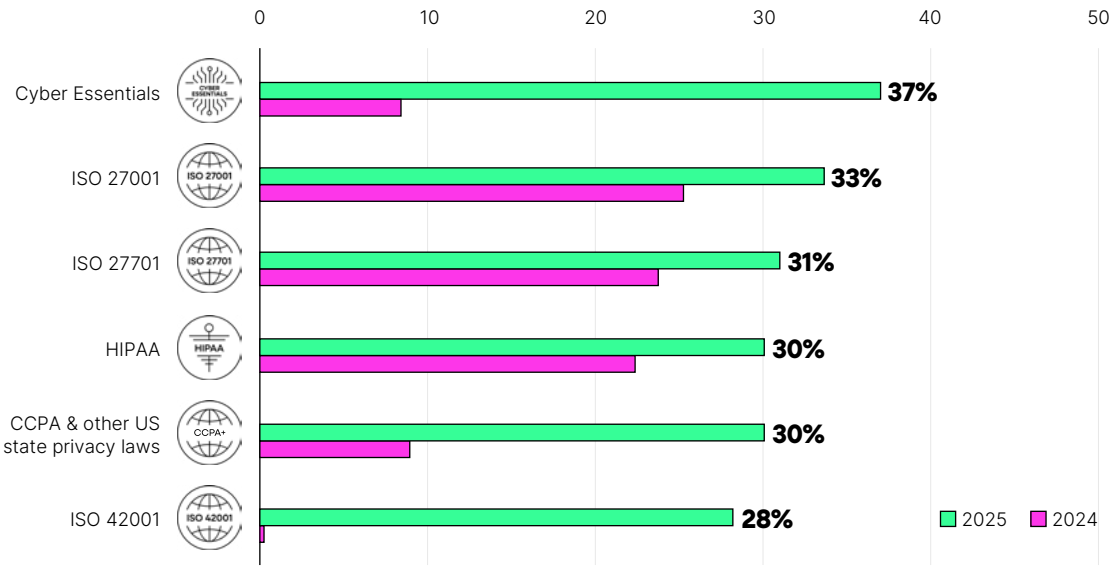


An increase in sales or business opportunities from new customers

With supply chain-related breaches continuing to make headlines, we're also seeing organisations implement more stringent compliance requirements for their suppliers. 37% of US respondents now require their suppliers to be certified to the UK government-backed cybersecurity baseline standard Cyber Essentials compared to 8% last year. A third (33%) require suppliers to be ISO 27001 certified, versus 25% last year.

Secure, compliant AI management is a priority, too. In a telling shift, over a quarter (28%) of organisations now require suppliers to be certified to ISO 42001, while less than one percent required this previously.

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



Addressing emerging risks

The pressure on organisations is compounded by emerging threats. Here, three key areas are top of mind for US respondents.

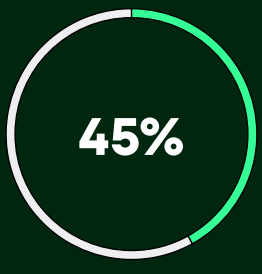
The Geopolitical Threat

As geopolitical tensions rise, nearly nine in ten (87%) US respondents are concerned about state-sponsored cyberattacks targeting their organisations. Key concerns include reputational risk if systems are compromised indirectly (44%) and operational disruption through supply chain impact (39%). As such, nearly all (98%) US organisations have proactively actioned incident response and recovery planning. 97% are investing strategically, taking a range of actions across the potential attack surface: threat intelligence; supply chain security and due diligence; increased board level engagement; security of cloud or data hosting locations; and vendor or supplier re-evaluation.

Incident response and recovery planning

Fully addressed | Significant action taken | Moderate action taken | Minimal action taken | No action taken

What action have you taken to address these threats?



Reputational risk if systems are compromised indirectly

Risk of operational disruption through supply chain impact

Increased threat landscape for our own systems

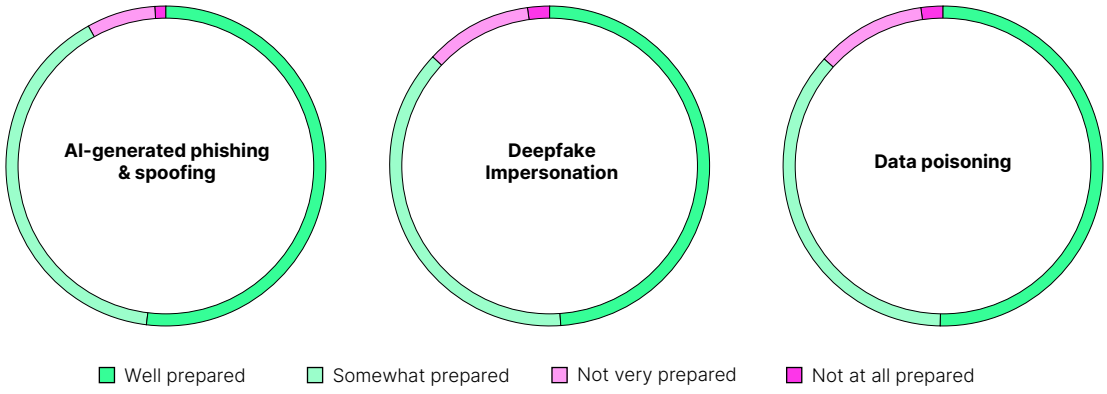
What concerns do you have about state-sponsored cyberattacks from a business perspective?

AI-Driven Attacks

As we mentioned previously, US respondents are most concerned about AI-powered threats over the next 12 months when it comes to emerging threats. AI-generated misinformation and disinformation, AI phishing, and shadow AI take the top three spots.

However, respondents are confident in their organisations' abilities to detect, defend against, and recover from AI-powered attacks. Over the next 12 months, many plan to invest in security technologies like GenAI threat detection and defence (97%), AI governance and policy enforcement (97%) and deepfake detection and validation tools (96%). Respondents feel most prepared to detect, defend against and recover from AI-generated phishing and spoofing, at 92%, and least prepared when it comes to AI data poisoning and deepfake impersonation, both 87%.

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

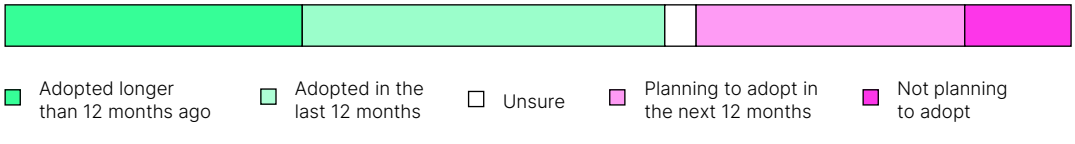


Quantum is Coming

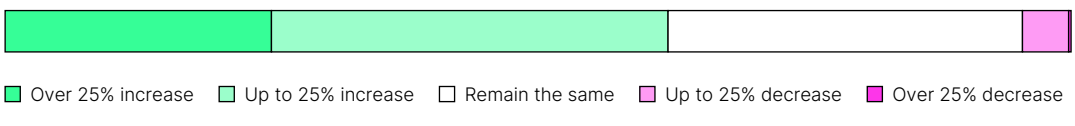
Quantum technology threatens to render many existing methods of encryption obsolete. It's also getting closer to becoming a more widespread reality – the National Institute of Standards and Technology (NIST) has released a set of encryption tools designed to withstand the attack of a quantum computer.

Our US respondents are taking proactive steps to protect their data. Three in five (61%) say they've adopted quantum computing-related security initiatives, while a further quarter (25%) are planning to do so in the coming 12 months. 93% plan to invest in quantum risk readiness over the next 12 months, and 61% expect to increase their spend on quantum computing security applications as they prepare to defend against quantum-based cyberattacks.

Have you, or do you plan 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?

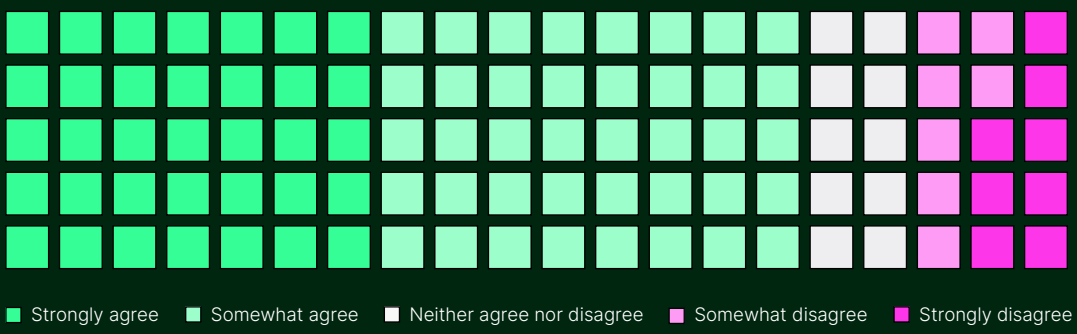


AI is a double-edged sword

The growing prevalence of AI is a double-edged sword for businesses. 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.

Nearly three in five (59%) organisations say AI and ML technologies are hindering their organisation's information security capabilities, likely due to the broadening attack surface and potential for innovative new AI-powered cyberattacks. Three quarters (76%) agree that advances in AI are beginning to blur the responsibilities and scope of traditional security roles, putting additional pressure on security teams to identify areas for AI use and areas where human insight is vital.

Perhaps unsurprisingly given the operational efficiencies and cost reduction AI technology offers, nearly two thirds (63%) of respondents say they adopted AI technology too quickly and are now facing challenges



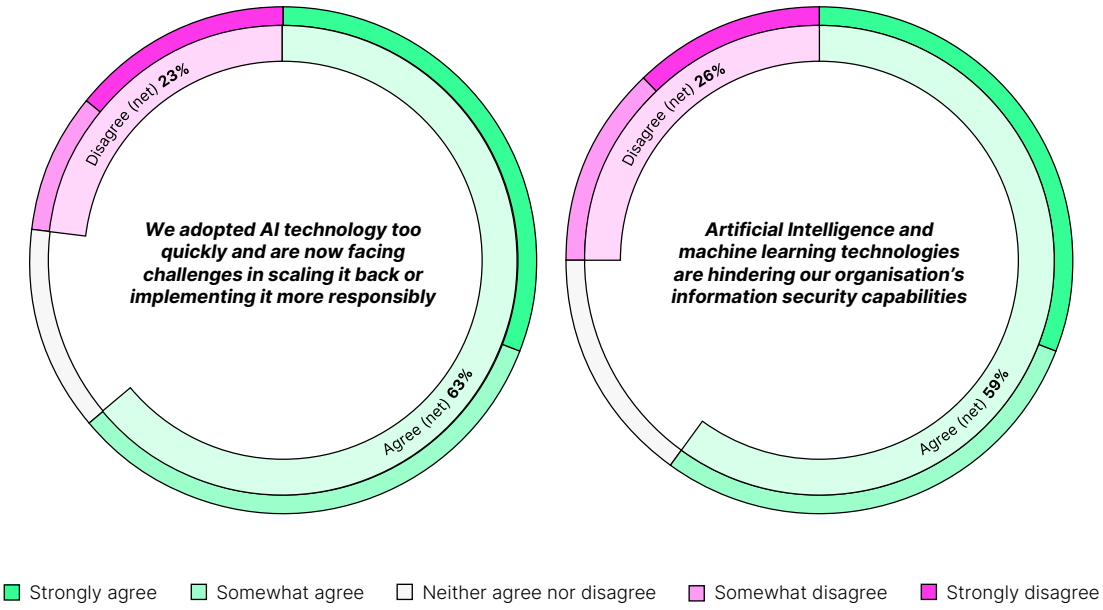
To what extent do you agree or disagree with the following statement: *Advances in AI are beginning to blur the responsibilities and scope of traditional security roles.*

in scaling it back or implementing it more responsibly. This is where the ISO 42001 standard comes in handy, providing a framework and guardrails for developing an ethical, secure AI management system (AIMS).

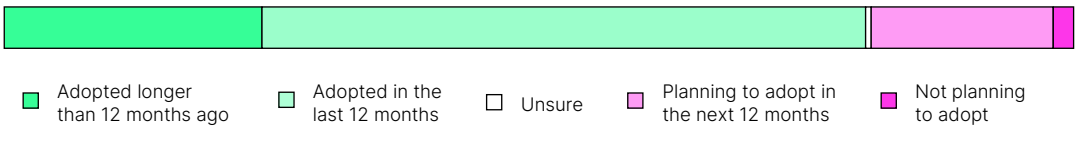
On the other side of the coin, four in five (80%) organisations have adopted AI, ML or blockchain technologies for security; a further 18% plan to adopt them in the next 12 months. If all goes to plan for these organisations, a solid 98% of our US respondents will have implemented AL, ML and blockchain security technologies by mid-2026, improving monitoring, task management, incident response capabilities and more.

If all goes to plan for these organisations, a solid 98% of our US respondents will have implemented AL, ML and blockchain security technologies by mid-2026

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



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?



‘*Unmanageable*’ supply chain risk

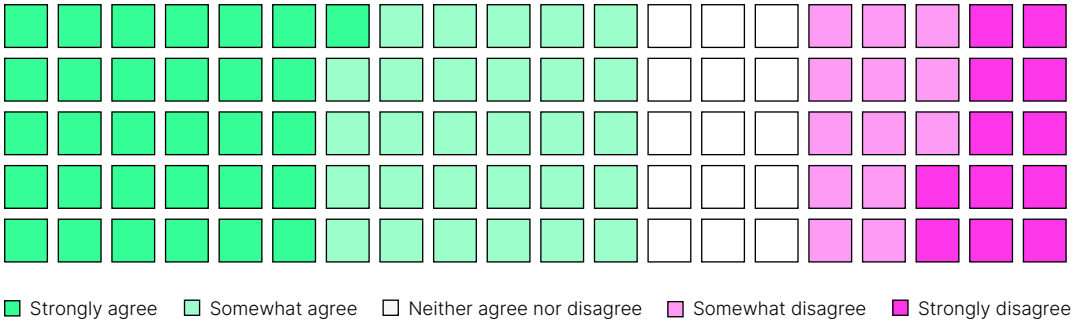
Supply chains are the backbone of modern business, yet they remain a persistent weak point in information security. With new regulations raising the bar, organisations must balance opportunity with the growing risks posed by third-party partners.

Supply chains have come under scrutiny in recent years, with many high-profile breaches caused by attackers exploiting organisations’ supply chain vulnerabilities to compromise their systems and access sensitive data. Securing the supply chain presents a challenge to one in three (34%) businesses. Two in three (66%) of our US respondents agree that security risks originating from third parties and supply chain partners are now “innumerable and unmanageable.”

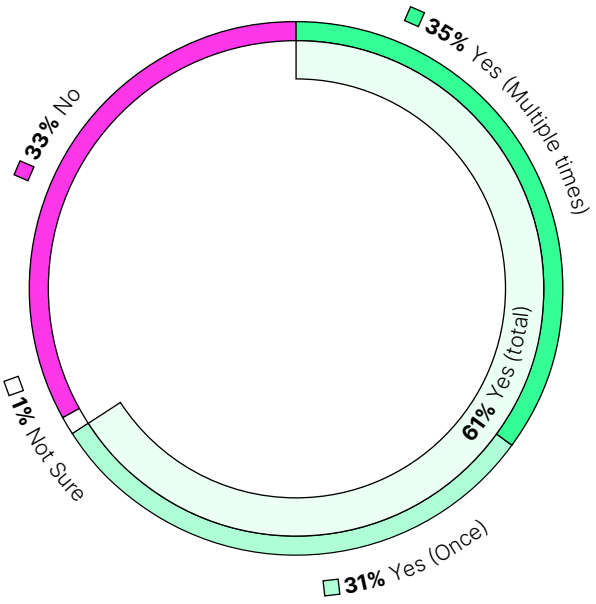
Two in three have also been impacted by a cybersecurity or information security incident caused by a supply chain partner or vendor in the past year; of those impacted, one in three experienced more than one incident. Affected organisations saw a range of repercussions, from data breaches affecting customers, employees or partners (43%) to financial loss or unplanned costs (37%), from increased scrutiny from regulators or auditors (36%) to temporary system outage or operational disruption (36%).

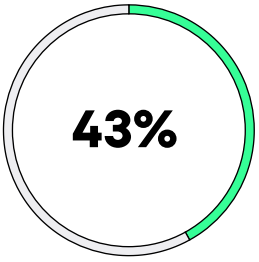
As a result, four in five (81%) organisations have strengthened their third party and vendor risk management, while another 16% are planning to do so in the next 12 months. Two thirds (66%) expect to increase their spend on supply chain and third-party vendor security.

To what extent do you agree with the following: *Security risks originating from third parties and supply chain partners are now innumerable and unmanageable.*

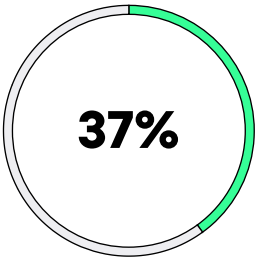


In the last 12 months, has your business been impacted because of a cybersecurity/ information security incident caused by a third-party vendor or supply chain partner?



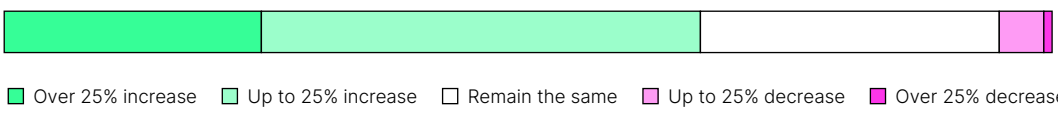


Resulted in a data breach affecting customers, employees or partners



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

How do you expect your company's spend in supply chain and third-party vendor security to change in the next 12 months?

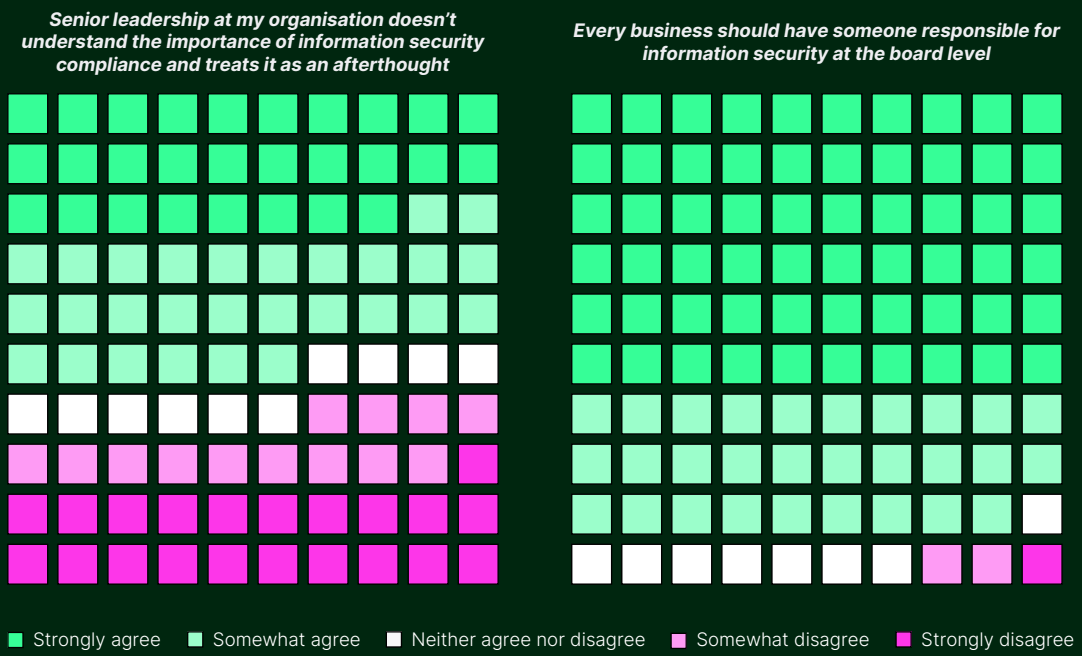


The importance of leadership buy-in

With the growing attack surface putting more pressure on security and compliance teams, information security professionals are pressing the need for board-level involvement, input and support.

Respondents are very clear that the responsibility for information security should not rest solely on the shoulders of the security team. 88% say every business should have someone responsible for information security at board level.

More than half (55%) say that senior leadership at their organisation don't understand the importance of information security compliance and treat it as an afterthought. However, 83% have improved visibility and reporting of security risks to leadership



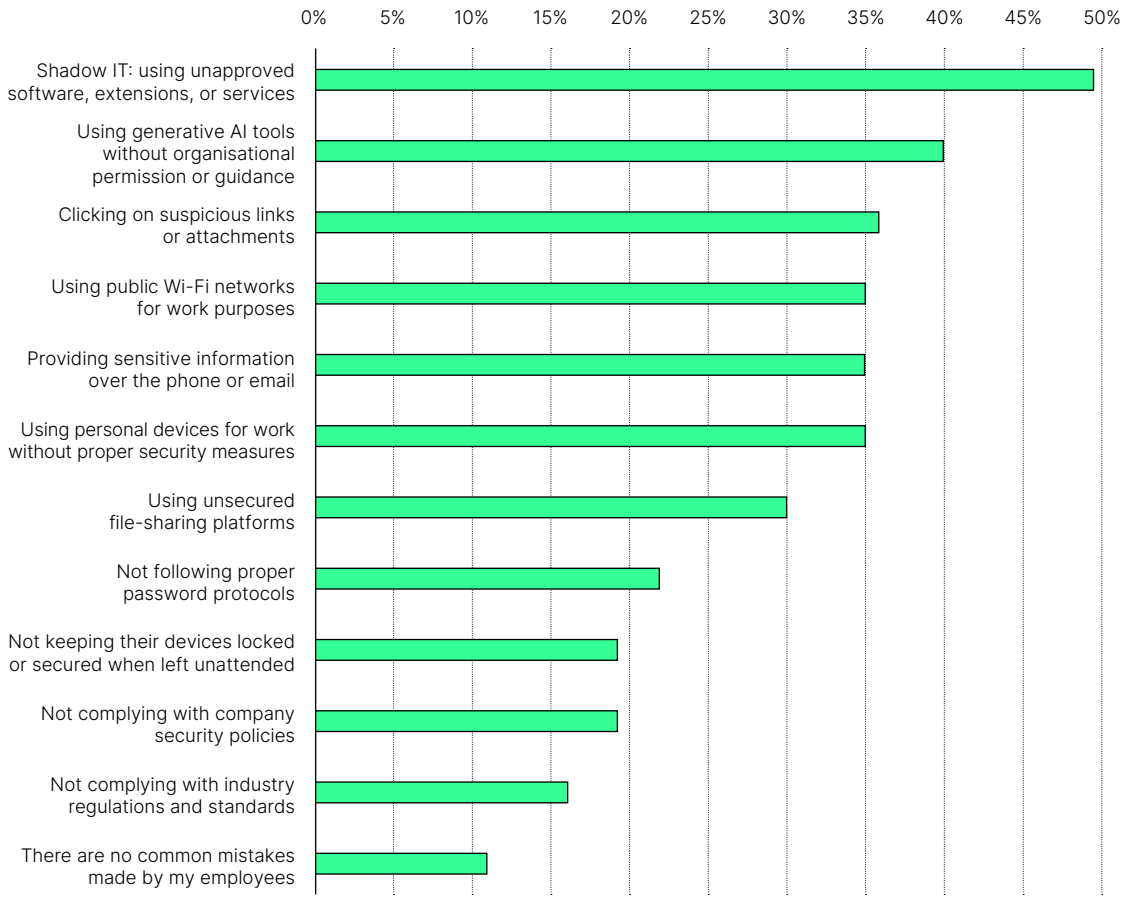
To what extent do you agree or disagree with the following statements about the current state of the information security landscape?

Leading from the front could mean the difference between a thwarted attack and a successful one

in the last 12 months, and 15% plan to do so in the next year. After all, information security risks are business risks, potentially impacting everything from reputation to new business wins.

Crucially, leadership buy in supports a culture of information security awareness. An engaged leadership team can help to ensure employees know their information security responsibilities as well as how to identify and report a potential attack. With nearly half (49%) of respondents reporting that employees engage in shadow IT use, 40% reporting shadow AI use, and 35% reporting that employees are still clicking on suspicious links or attachments, leading from the front could mean the difference between a thwarted attack and a successful one.

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



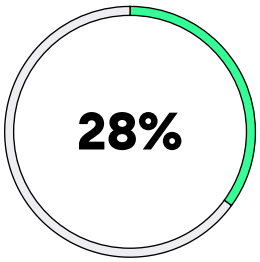
Looking ahead

Given the challenges and opportunities, they're facing in equal measure, what are US organisations' security priorities for the next 12 months?

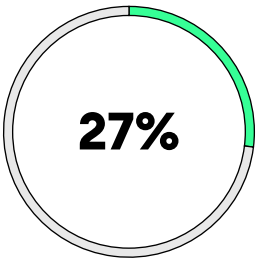
Respondents are firmly focusing on AI risk management: 28% say they're enhancing defences against AI-generated threats like phishing and deepfakes. 27% are improving their ability to authenticate digital communications and detect manipulation. Employee training is another top priority, with 26% focusing on enhancing employee security awareness and behaviour. Supplier management is also top of mind; nearly a quarter (24%) are prioritising strengthening third party and vendor risk management.

AI remains the top priority when we look at organisations' plan for security investments. Nearly all (97%) plan to invest in GenAI threat detection and defence, supporting their confidence in being able to detect, respond to and recover from these attacks. 96% plan to invest in AI governance and policy enforcement; the same number plan to invest in deepfake detection and validation tools.

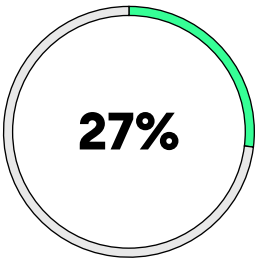
What are your organisation's top information security priorities for the next 12 months?



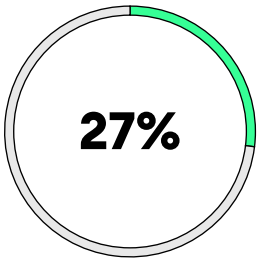
Enhancing defences against AI-generated threats



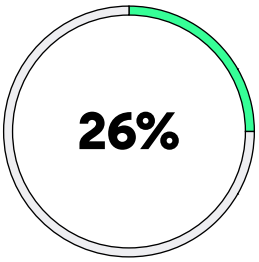
Improving incident response preparedness and recovery capabilities



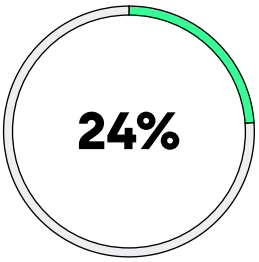
Improving ability to authenticate digital communications and detect manipulation



Improving incident response preparedness and recovery capabilities

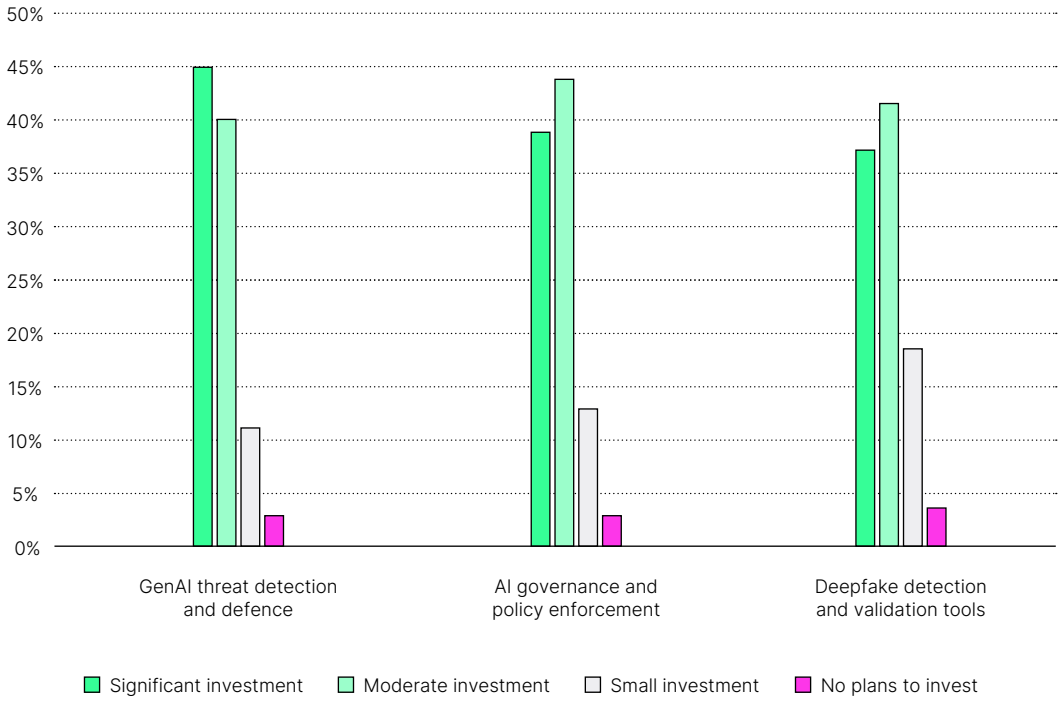


Enhancing employee security awareness and behaviour



Strengthening third-party and vendor risk management

How much, if any, do you plan to invest in the following emerging security technologies in the next 12 months?



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

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.

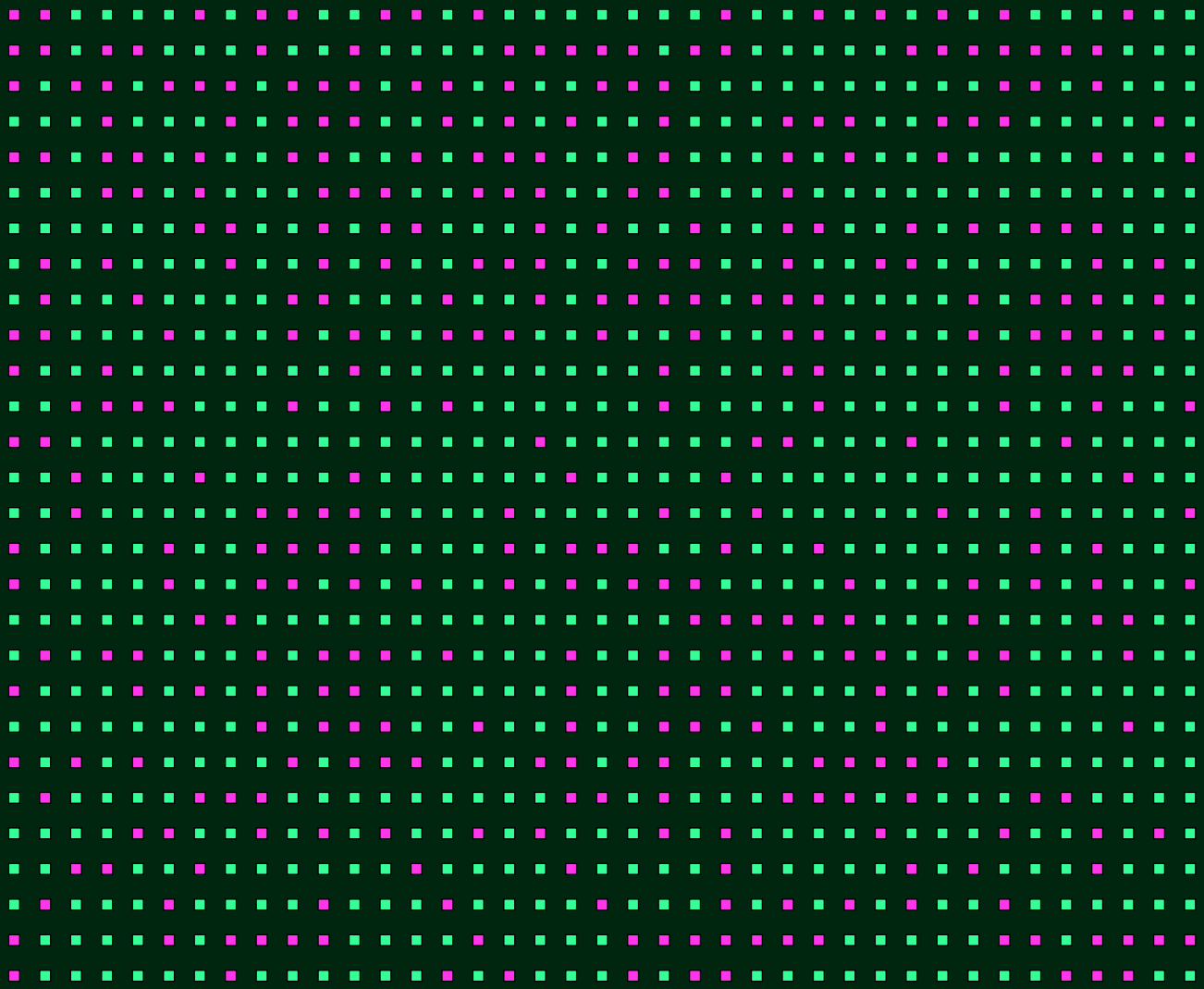
This year's research makes one thing clear: compliance is now central to security strategy. Three in four US organisations received fines for non-compliance in the last year, and over a third of those penalties were more than $330,000. More than two-thirds of respondents told us they struggle to manage 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, reduce 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**