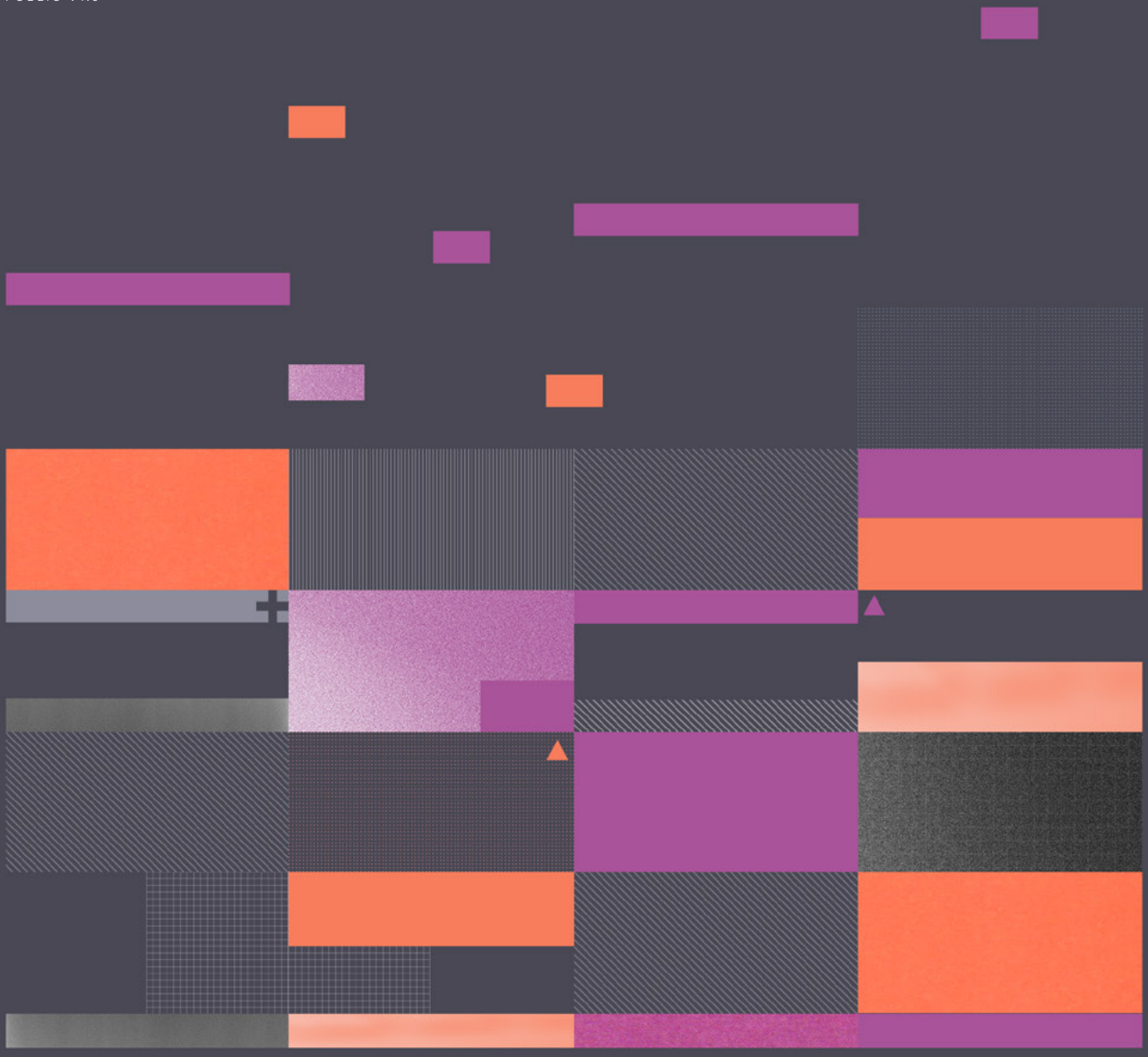
isms.online

THE STATE OF INFORMATION SECURITY REPORT 2024

THE IMPACT OF INFORMATION SECURITY ON BUSINESS RESILIENCE AND SUCCESS

PUBLIC V1.0



CONTENTS

EXECUTIVE SUMMARY

LUKE DASH
CEO, ISMS.ONLINE

NAVIGATING THE NEW FRONTIERS OF INFORMATION SECURITY

This year's report, reflecting contributions from over 1,500 information security professionals across the UK, USA, and Australia, underscores a pivotal evolution in the information security landscape.

Amidst the rapid technological advancements and shifts in the global business environment, our findings highlight the profound impact of information security on business resilience and success.

In the current climate marked by economic uncertainty and relentless digital transformation, the role of robust information security practices has transitioned from being a preventive measure to a fundamental driver of business growth. The report reveals that organisations that deeply integrate information security into their operational ethos enhance their defence against cyber threats and strengthen their market position, ultimately achieving significant competitive and financial advantages.

Organisations that deeply integrate information security into their operational ethos enhance their defence against cyber threats and strengthen their market position, ultimately achieving significant competitive and financial advantages

This year, 38% of respondents highlighted managing third-party and vendor risks as businesses' most significant challenges. This is a direct consequence of expanding digital ecosystems and increasingly interconnected business operations. Effective management of these risks is crucial for minimising the attack surface and ensuring the integrity and reliability of business operations. Compliance with diverse regulations remains a close second, cited by 33%, reflecting the intricate patchwork of international and domestic laws that organisations must navigate.

Amid these challenges, AI emerges as both a vector of risk and a transformative tool for enhancing security operations. While only a quarter of organisations have adopted new AI technologies within the year, a significant majority acknowledge their potential to improve security outcomes. This potential is particularly notable in addressing the pervasive skills gap within the industry, with AI

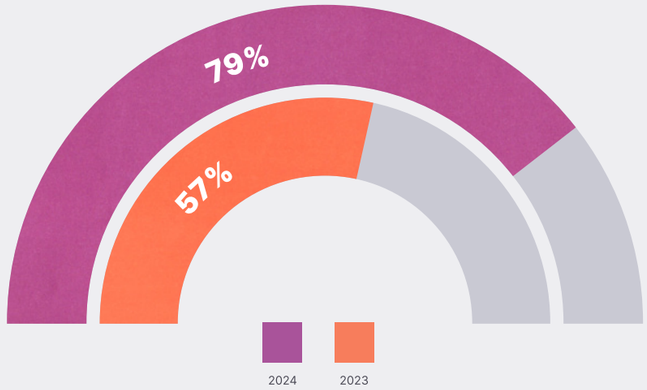
Companies that invest in advanced security measures and compliance reduce their exposure to cyber threats and see tangible benefits regarding operational efficiency, customer trust, and financial outcomes.

poised to augment capabilities in security operations centres and enhance threat detection and response.

Our research also points to the escalating challenge posed by sophisticated cyber threats, including the rise of AI-powered attacks such as deepfakes and advanced phishing scams. These threats are becoming more prevalent and are exploiting gaps in traditional security frameworks, which many businesses are struggling to address swiftly and effectively. The report also reveals a worrying trend in data breaches, especially involving partner and financial data, which are the most frequently compromised data types.

ISO 27001 continues to be a critical standard for organisations, aiding in the structuring and streamlining of information security management. Compliance with such standards helps businesses mitigate risks and enhances their reputation as secure and reliable operators.

This year's findings highlight the intrinsic link between robust information security and business performance. Companies that invest in advanced security measures and compliance reduce their exposure to cyber threats and see tangible benefits regarding operational efficiency, customer trust, and financial outcomes.



79% OF BUSINESSES HAVE BEEN IMPACTED BECAUSE OF AN INFORMATION SECURITY INCIDENT CAUSED BY A THIRD-PARTY VENDOR OR SUPPLY CHAIN PARTNER, AN INCREASE OF OVER 20% FROM LAST YEAR

70%

OF BUSINESSES HAVE RECEIVED FINES FOR DATA BREACHES IN EXCESS OF £100,000 IN THE LAST 12 MONTHS

£258k

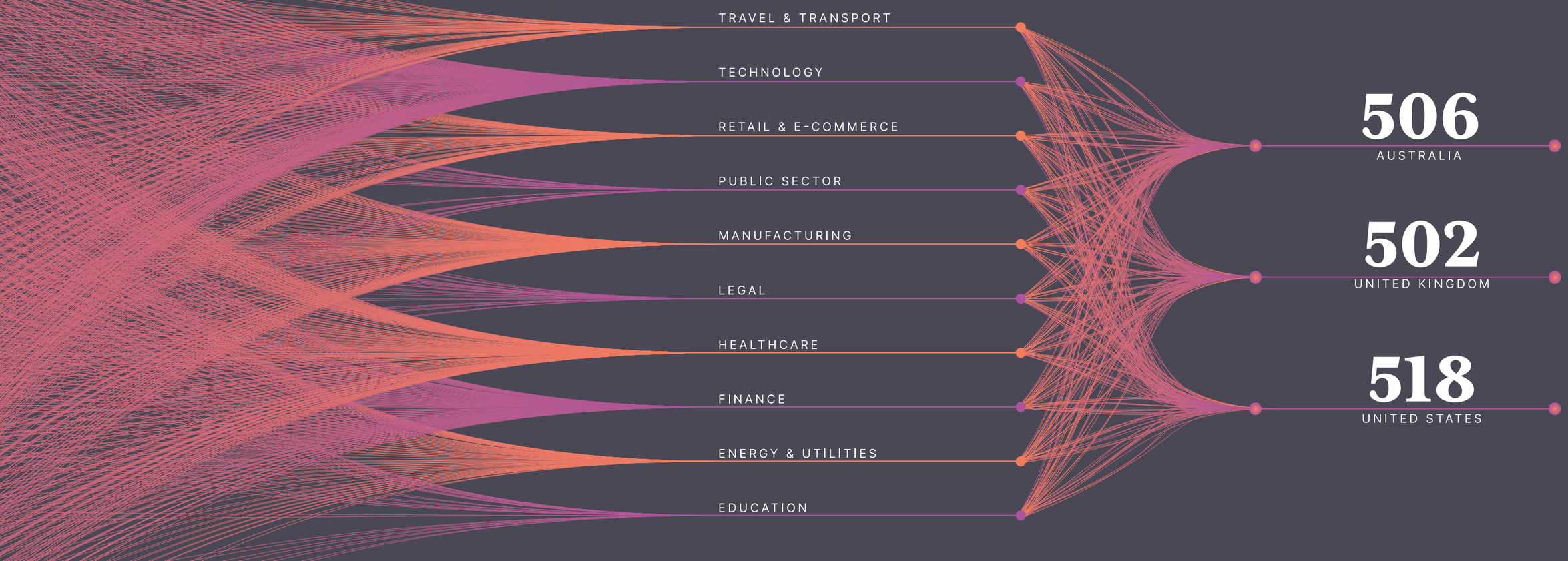
THE AVERAGE FINE AMOUNT BUSINESSES ARE REPORTING HAS INCREASED 3.5% IN JUST ONE YEAR TO £258,000

DEEPFAKES ARE THE SECOND HIGHEST CYBER SECURITY INCIDENT EXPERIENCED BY BUSINESS IN THE LAST 12 MONTHS

ABOUT THE REPORT

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 inaugural report, which canvassed the opinions of only UK respondents, this year we polled 1526 respondents who work in information security across the UK, USA and Australia.

Their responses have helped us to uncover the main information security and compliance challenges facing organisations in these regions, the impact of AI on the landscape, and how they are driving business value and ROI from compliance. We thank them for their invaluable input.



ABOUT THE AUTHOR

Phil Muncaster has been an IT journalist for 15 years. He 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 now regularly contributes to the ISMS.online blog.

01

CHARTING TODAY'S RISK LANDSCAPE

Today's business and IT leaders are caught in a bind. First came the pandemic, then the persistent economic and macro-uncertainty of the years that followed. Against this backdrop, they know that digital transformation is the best way to drive the process efficiencies, business agility and data-driven customer insight needed for sustainable growth. And they know that to truly prosper, they must make the most of dynamic partnerships with third-party suppliers and specialists – from open source developers to business process outsource (BPO) firms.

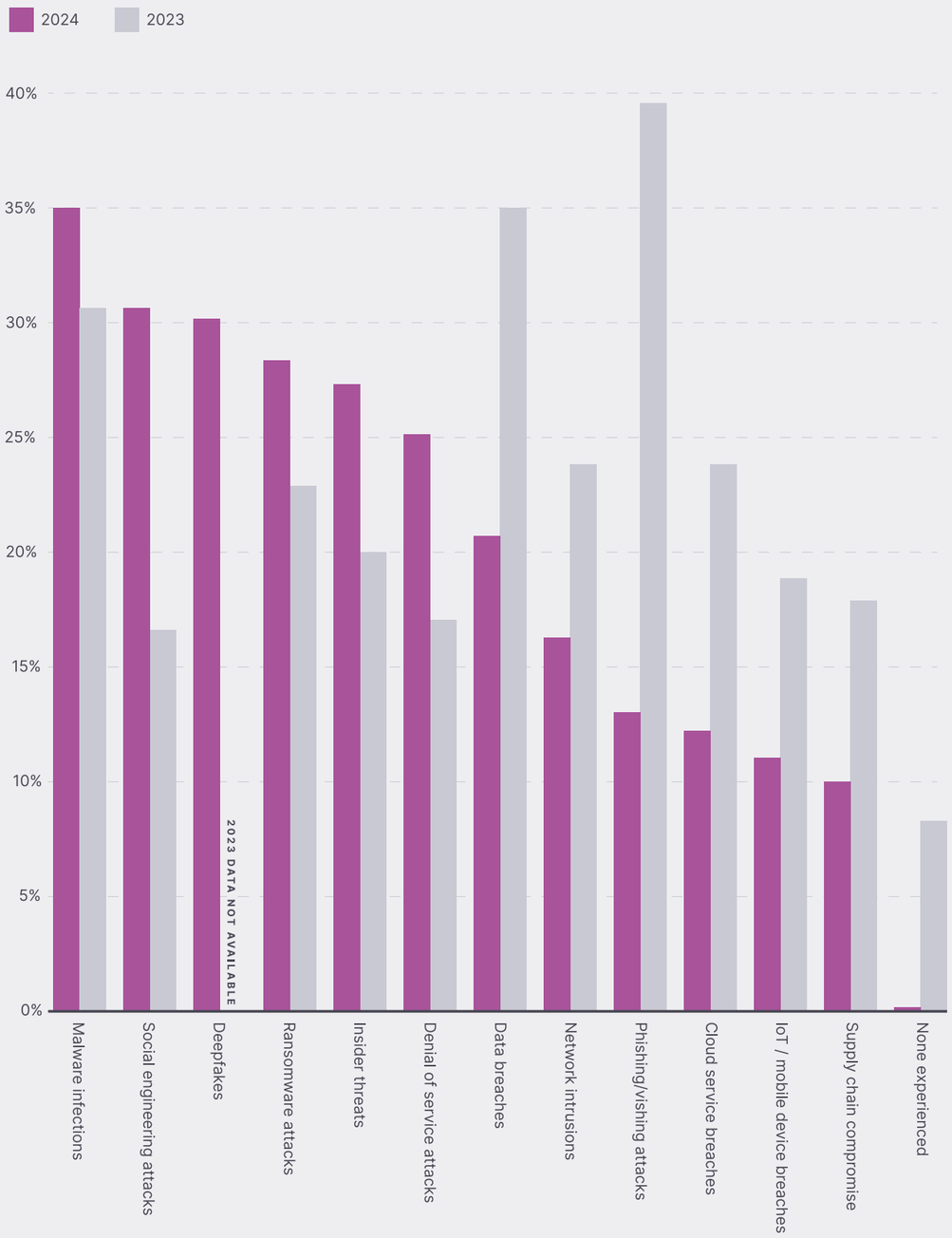
With each new investment and supplier, they are most likely also expanding the digital attack surface. This explains why managing vendor and third-party risk is the biggest challenge facing global respondents.

But with each new investment and supplier, they are most likely also expanding the digital attack surface. This explains why managing vendor and third-party risk is the biggest challenge facing global respondents (38%). And why managing and securing IoT and BYOD devices (30%) also appears in the top five. As much as theses investments offer in business value, that value can only be realised if risk is properly managed.

Of course, regulators know this, which is why organisations across the UK, US and Australia must comply with a patchwork of overlapping industry-specific and domestic and international rules. Yet the complexity of these requirements can also undermine regulators' efforts to improve baseline best practices and safeguard the public. It's why compliance with regulations and industry standards was the second top information security challenge cited by respondents (33%).

WHAT ARE THE CHALLENGES YOU ARE CURRENTLY FACING IN INFORMATION SECURITY?

WHAT TYPES OF CYBER SECURITY / INFORMATION SECURITY INCIDENT HAS YOUR BUSINESS EXPERIENCED IN THE LAST 12 MONTHS



02

THREAT ACTORS ARE RELENTLESS AND INNOVATIVE

All of which has not gone unnoticed among financially motivated cyber-criminals and emboldened nation state actors – who are past masters at probing for security gaps and exploiting weaknesses in capacity. Over the past 12 months, the biggest impact of their efforts has been in malware infections, cited by 35% of respondents. The figure is even higher (47%) in the tech sector – so often a target for such attacks.

Malware is increasingly packaged up in "as-a-service" offerings that deliver everything a threat actor needs to compromise their target. The end result could be anything from cryptocurrency mining and network access, to full system encryption and sensitive data/credential theft. In fact, data breaches (22%) and ransomware attacks (29%) are also high on our list of top security incident last year – highlighting the interlinked nature of such threats.

It will come as no surprise that threat actors continue to target employees. A third (32%) of respondents say they experienced social engineering attacks over the past 12 months. And 28% cite insider threats, which can be the result of malicious but also negligent employees.

In this context, improved training and awareness raising is critical. But even the best trained staff may have trouble spotting deepfakes. Attacks featuring the AI-powered technology are cited by 30% of respondents – a worryingly high share. It appears that voice and video-cloning tech is already becoming cheap and convincing enough for threat actors to try it. The most likely scenario today is use in business email compromise (BEC)-style attempts to trick recipients into making corporate fund transfers. But there are possible use cases for information/credential theft, reputational damage or even to bypass facial and voice recognition authentication.

Attacks featuring deepfakes are cited by 30% of respondents. It appears that voice and video-cloning tech is already becoming cheap and convincing enough for threat actors to try it.

Whatever the threat, the end result for organisations could be severe: significant data loss and/or service outages resulting in severe financial and brand damage.

Partner data (41%) is cited more than any other as being compromised – highlighting the persistent risks posed by suppliers. Could it be that this data is typically less well-secured in many organisations?

03

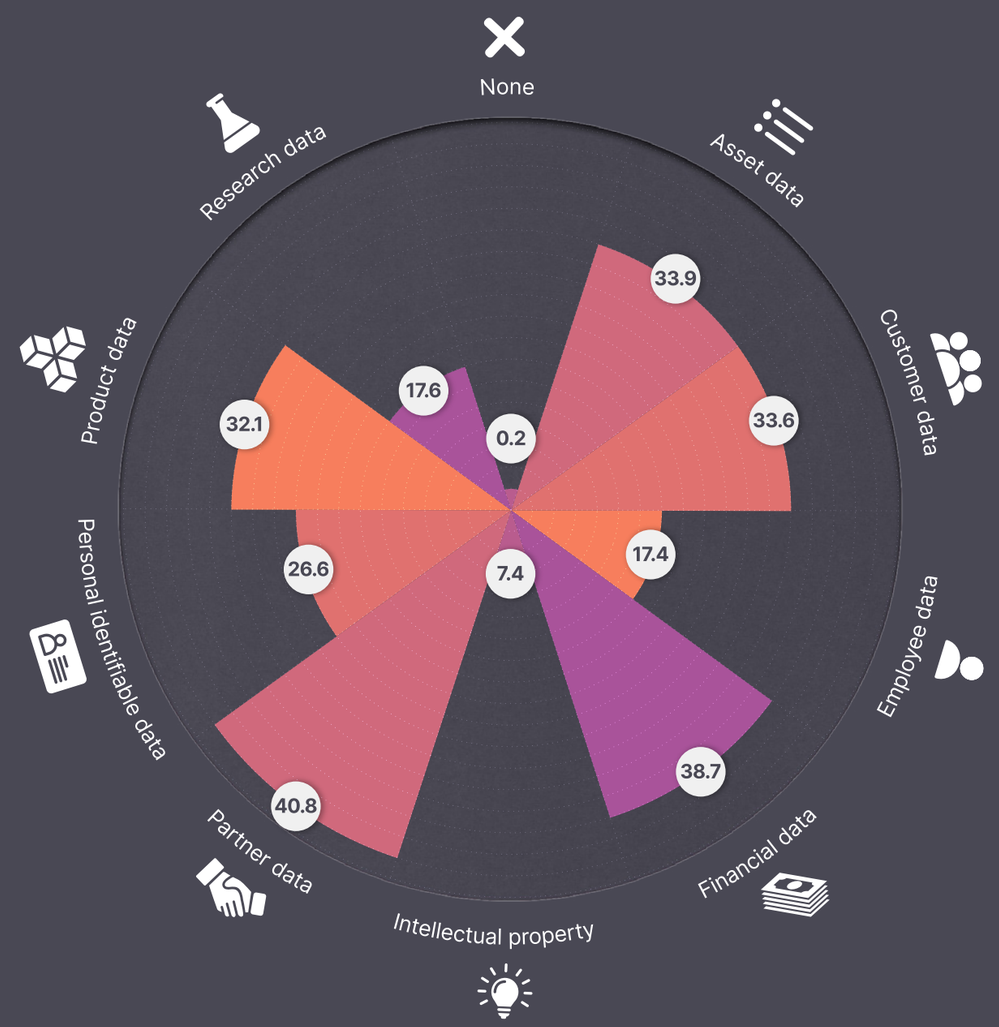
DATA THEFT UNDER THE RADAR

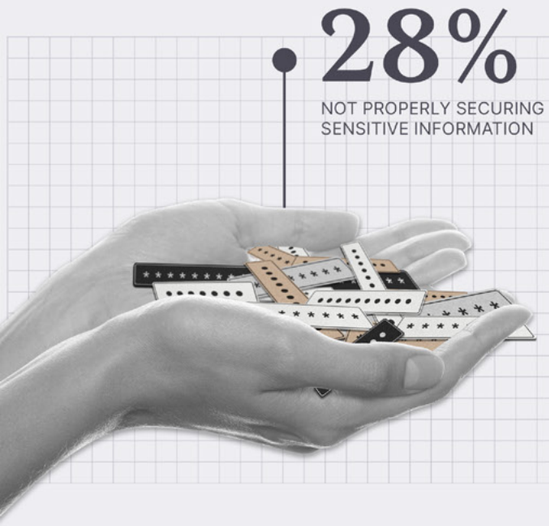
Data remains arguably the most valuable commodity an organisation holds. It's why regulations like the GDPR have set such a high bar for protecting and handling this information securely. It's also why threat actors are so keen to get their hands on it – whether it's to monetise for fraud and extortion, or to use for geopolitical and/or strategic ends.

Partner data (41%) is cited by more of our respondents than any other as being compromised in the past 12 months – highlighting the persistent risks posed by suppliers. Could it be that this data is typically less well-secured in many organisations? It's also notably less of an issue for retailers (27%) but much more likely to impact tech sector respondents (55%).

Perhaps unsurprisingly, financial data (39%) came second, with asset (34%) customer (33%) and product (32%) data not far behind. PII came some way behind (27%), which is somewhat surprising, considering it is often one of the key targets in ransomware – which continues to impact a large number of organisations of all sizes and sectors. It should be noted, however, that this data type is more likely to be cited as compromised by energy & utilities (38%) and retail (35%) sector respondents.

WHAT TYPES OF DATA, IF ANY, HAVE BEEN COMPROMISED IN YOUR BUSINESS IN THE LAST TWELVE MONTHS





28%
NOT PROPERLY SECURING SENSITIVE INFORMATION

27%
CLICKING ON SUSPICIOUS LINKS OR ATTACHMENTS

22%
USING PUBLIC WI-FI NETWORKS FOR WORK PURPOSES

35%
USING PERSONAL DEVICES FOR WORK PURPOSES WITHOUT PROPER SECURITY MEASURES

WHAT ARE THE COMMON TYPES OF INFORMATION SECURITY/ CYBER SECURITY MISTAKES MADE BY YOUR EMPLOYEES?

04 PEOPLE REMAIN A CRITICAL INFOSECURITY CHALLENGE

There are two ways to view an organisation's employees. On the one hand, they can be a fantastic first line of cyber defence. Yet too often they are also a weak link in the security chain. That would explain why social engineering and phishing remain top challenges for respondents, as threat actors relentlessly try to force the errors which could given them access to corporate networks.

Yet just 12% of overall respondents say a lack of staff awareness around current information security risks is their biggest challenge. Could this be a sign that their training initiatives are working? Nearly half (45%) of respondents claim they've adopted a greater focus on employee education in the past year, the number one answer. It rises to 58% in the tech sector and 50% among utilities respondents.

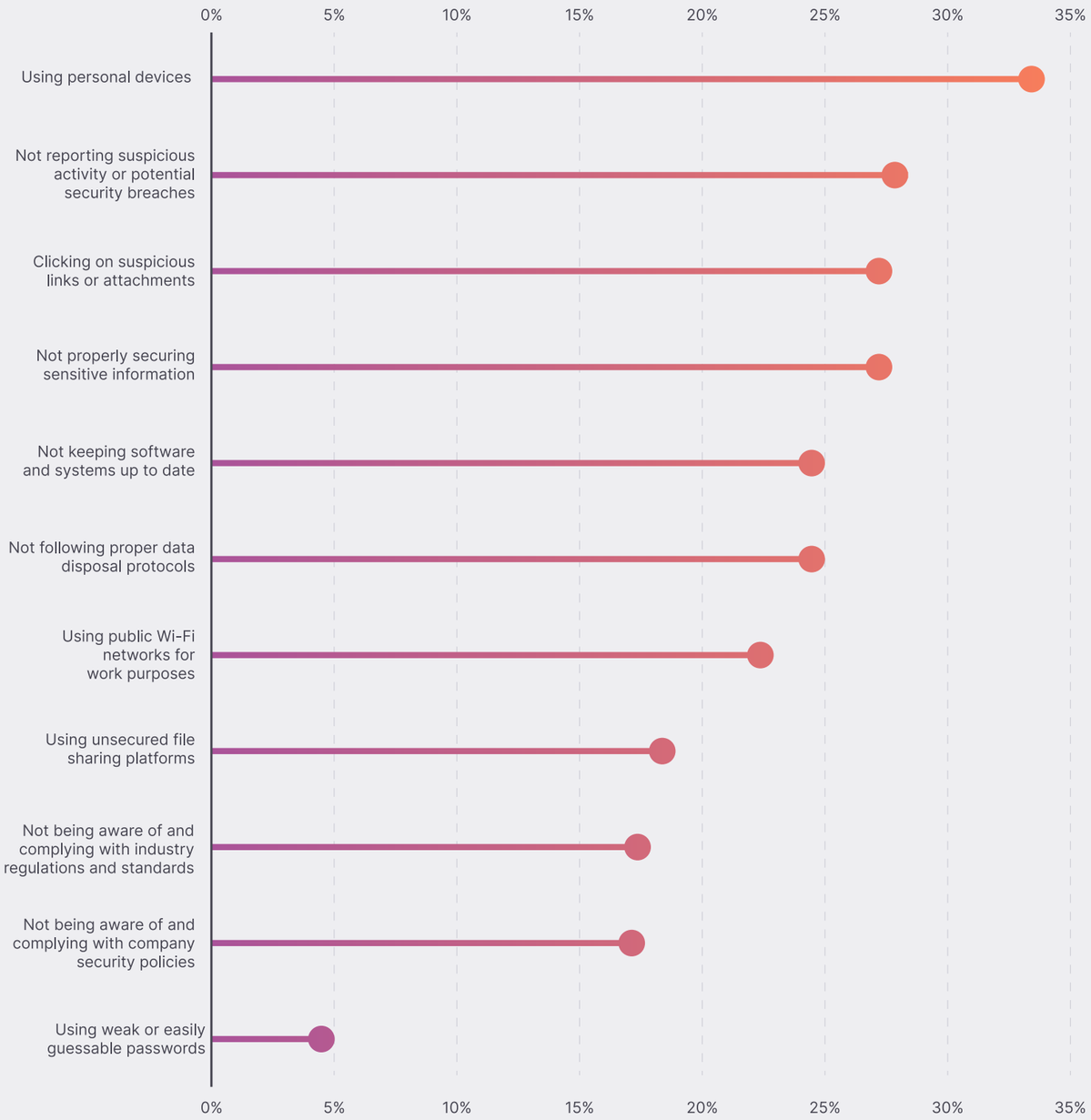
Just 12% of respondents say a lack of staff awareness around current information security risks is their biggest challenge. Could this be a sign that their training initiatives are working?

It's reassuring to hear that employee awareness is so low down on the list of respondents' challenges, although it flies on the face of countless other studies over the past year. Nevertheless, as threats continue to evolve, so must education programmes.

As to where they should focus, the research finds that using personal devices for work purposes without proper security measures is the number one type of mistake made by employees over the past year (35%). This speaks to the reality of the modern workplace, where many employees now log-on remotely or work in a hybrid setup. A much smaller share of public sector respondents (16%) cite this as a common employee mistake, perhaps because fewer staff are allowed to use their own devices for work. Conversely, in the tech sector (52%) it's much higher.

Whether they're using a smartphone, tablet, laptop, or even a home desktop, there are several red flags: including a lack of proper patching (cited by 25% of respondents),

WHAT ARE THE COMMON TYPES OF INFORMATION SECURITY/ CYBER SECURITY MISTAKES MADE BY YOUR EMPLOYEES?



It's somewhat reassuring that password best practice is improving. Just 5% of respondents claim their staff used weak easily guessed passwords in the past year.

unsecured home networks, or even use of devices on public Wi-Fi networks (cited by 22%). These environments are a boon for threat actors, as it is often fairly straightforward to circumvent security controls – and from there, to eavesdrop on other network users, steal corporate logins and access trusted environments. It's part of the reason that zero trust approaches have gained so much traction in recent years.

Although these risks are not confined to home and remote users, there's a strong case for saying that employees are more likely to engage in risky behaviour like clicking through on phishing links (cited by 28%, rising to 44% in pub sector), or using unsecured file sharing services (19%) when away from the office. And perhaps they're less likely to report suspicious activity or potential security breaches – an issue cited by 29% of respondents. It's absolutely critical for staff to do this – to ensure that IT teams understand the level of risk facing their organisation and can take prompt action. This is where good training can turn employees into a much-needed early warning system for threats.

It's somewhat reassuring that password best practice is improving. Just 5% of respondents claim their staff used weak easily guessed passwords in the past year. And only 1% claim employees provided sensitive information over the phone without proper authentication. The caveat here is if this 1% includes the IT helpdesk or a key call centre operative, it could still lead to a major breach. Increasingly, advanced threat groups are using voice phishing/social engineering techniques on hand-picked targets as part of SIM swap fraud campaigns or to gain initial access for ransomware.

05

SPENDING IS SURGING IN A BID TO IMPROVE SECURITY AWARENESS

The good news is the UK, US and Australian organisations are largely increasing their budgets for employee cybersecurity awareness and training programmes. Overall, 40% expect their budget to increase by up to a quarter in the next 12 months, and a further fifth (20%) claim it is going up by over 25%. But it's critical that this money is spent effectively.

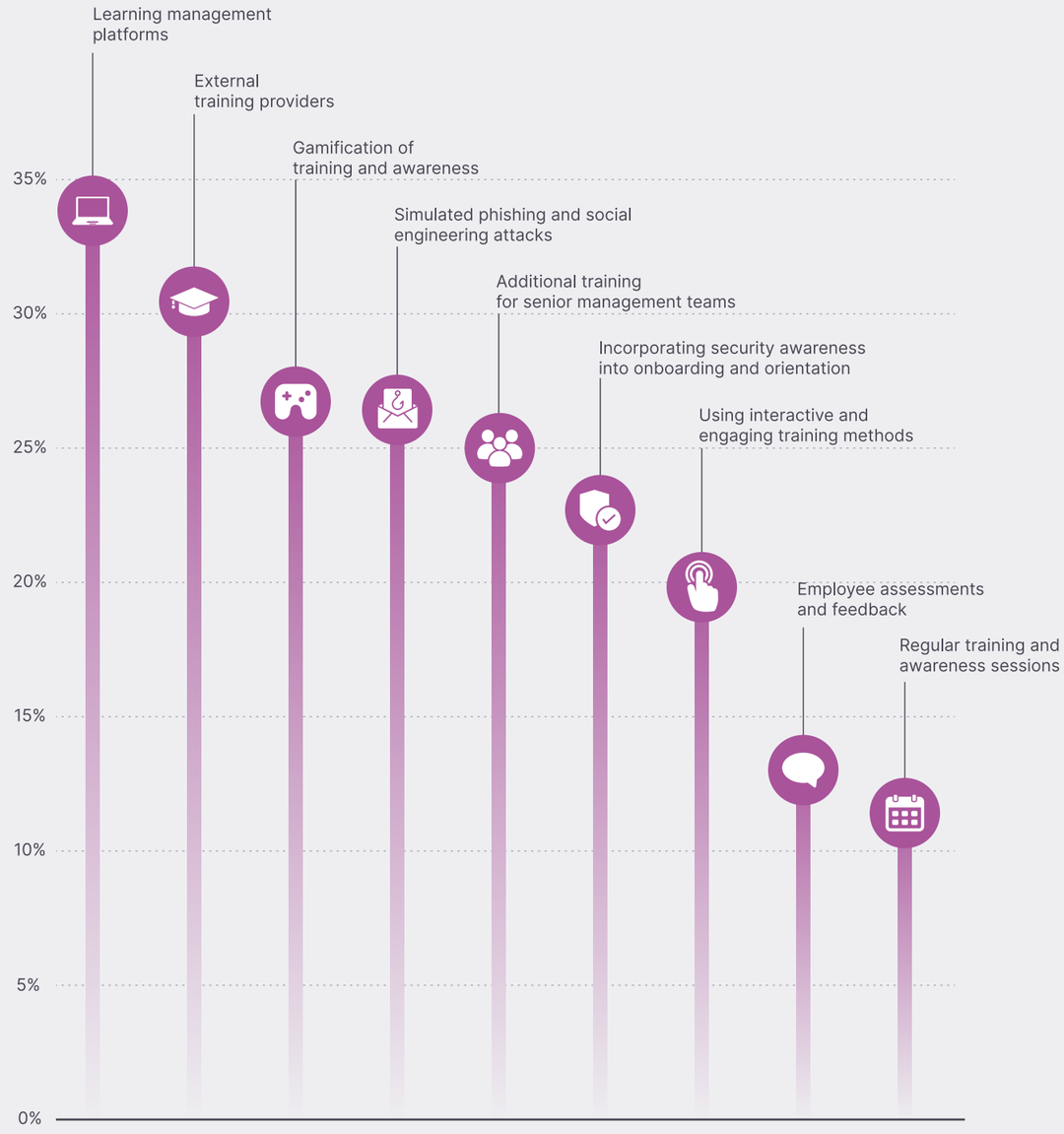
Our research reveals that the training methods thought to be most effective are learning management platforms – cited by 35%, rising to 46% of tech sector respondents. In fact, IT security leaders are spoiled for choice when it comes to digital resources that can help them. Perhaps most important is that they run lessons "little and often" to maximise the chance of new information actually changing behaviours. In fact, 14% cite regular sessions as important.

Simulations (cited by 27%) are also a great idea to immerse employees into the world of phishing – exposing them to realistic-looking attacks. Ideally, such simulations would also have a high degree of personalisation, to enable frequent updates reflecting the latest scams. Gamification (cited by 28%) has also been proven to work on employees, to increase the chance of lessons hitting home.

Those at the top of the organisation may benefit from extra sessions, as these high-profile, time-poor targets are often singled out by threat actors.

Finally, it's important that every staff member – including part-time employees and contractors, all the way to senior management – is included in training programmers. In fact, those at the top of the organisation may benefit from extra sessions, as these high-profile, time-poor targets are often singled out by threat actors. Over a quarter (27%) of respondents say additional training for senior management has proven most effective.

WHICH METHODS OF IMPROVING SKILLS AND AWARENESS HAVE PROVEN TO BE MOST EFFECTIVE IN YOUR BUSINESS?



31%

OF RESPONDENTS CITED INFORMATION SECURITY SKILLS GAP AS A TOP CHALLENGE THEY ARE CURRENTLY FACING

06

ADDRESSING THE CHRONIC INDUSTRY SKILLS GAP

The human-shaped challenge in information security also extends to the security team itself. That's due to significant skills gaps and shortages that have persisted for years. The challenge is partly one of perception: historically, children have come to view IT and cybersecurity as a geeky and technically complex career. That puts many off progressing with the academic qualifications that can act as a springboard for career development. Another factor is its perception as a predominantly white and male-dominated industry – one that unfortunately has a ring of truth to it.

Now that many professionals are retiring without enough younger entrants taking their place, there is genuine concern over the impact of such shortages.

Now that many professionals are retiring without enough younger entrants taking their place, there is genuine concern over the impact of such shortages. In fact, our research reveals that the information security skills gap is a top-three challenge for respondents, cited by 31% and rising to 47% in both the public and education sectors. Neither can afford to remain short-staffed, as critical threats continue to emerge and digital investments continue to grow organisations' attack surfaces. In fact, the global skills shortage today stands at four million professionals, including 73,400 in the UK, 483,000 in the US and 28,000 in Australia, according to one estimate.

This shortfall is perpetuated by poor recruitment that fails to tap a potentially large

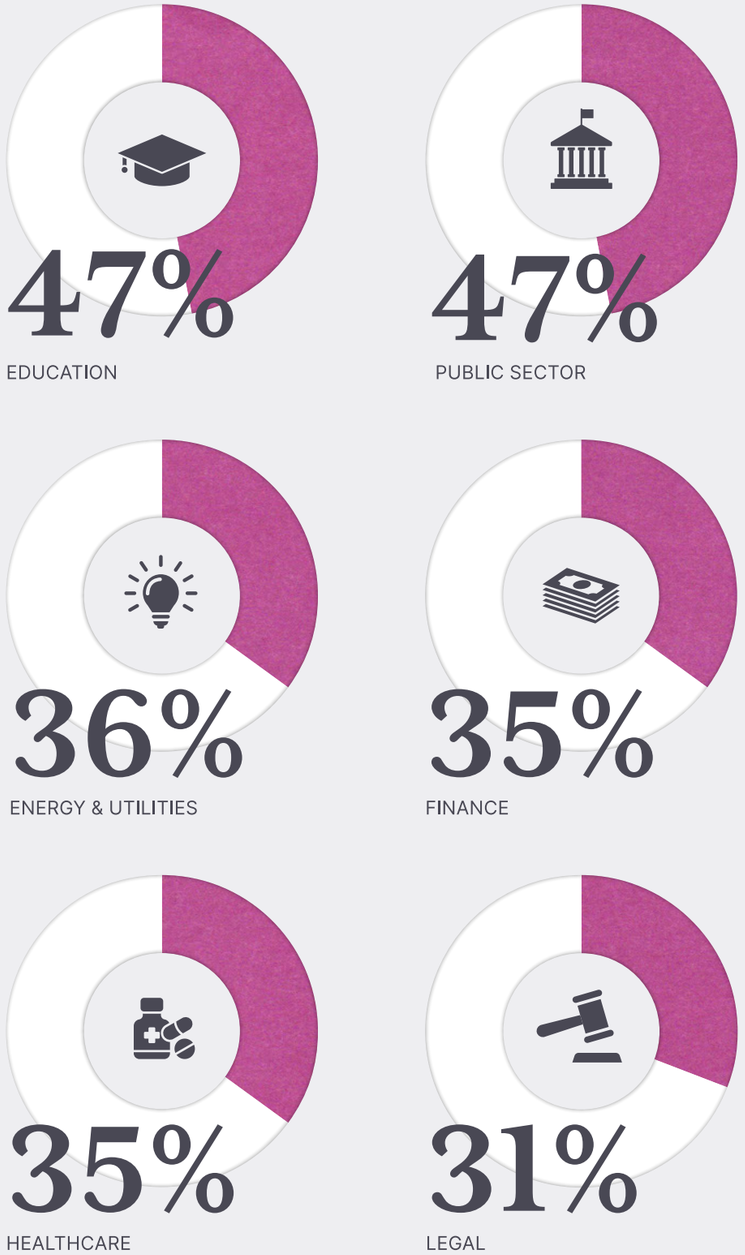
The global skills shortage today stands at four million professionals, including 73,400 in the UK, 483,000 in the US and 28,000 in Australia, according to one estimate.

pool of talent. Government strategies continue to try and fill the pipeline by encouraging younger people to take an interest in the subject at school. In time they may bear fruit. But in the meantime, recruiters could help increase the talent pool by putting less weight on academic qualifications and industry certifications, and more on transferable skills and natural aptitude.

A broader approach – including community outreach projects – could also help to address the diversity challenge the industry still has. Candidates from adjacent industries and in adjacent roles could be approached to retrain. And sponsorship of apprenticeships and scholarships would help to fill the talent pipeline. It's reassuring to see a majority of respondents plan to increase investment in recruiting and hiring for cybersecurity teams over the coming year. Some 37% claim they'll increase investment by 25% and a further quarter (25%) will ramp up spending by over 25%.

Another factor perpetuating skills shortages in the UK, US and Australia is thought to be employee burnout. However, some good news from this research is that doesn't seem as prevalent as other industry snapshots would have us believe. It could be perhaps that where burnout happens, it is focused in specific niche roles in cyber like SOC analysts. Overall, only 3% of those surveyed consider staff turnover and burnout a challenge, dropping under 2% for respondents in the UK. It appears that historically low unemployment rates in sector and healthy average salaries may be encouraging most professionals to stay put.

SECTORS FEELING THE STRAIN OF THE CYBER SKILLS GAP



07

SUPPLY CHAINS CREAKING UNDER THE PRESSURE OF CYBER RISK

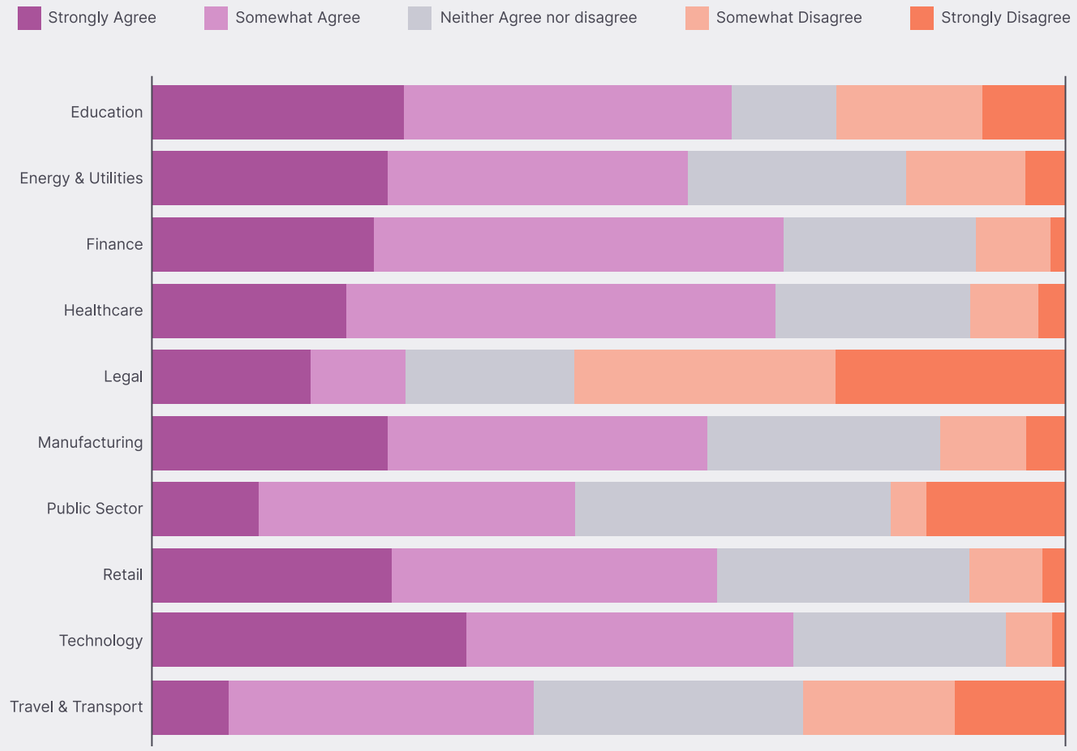
Supply chains are the glue that hold together global commerce. They form an increasingly complex web of interlinked relationships which see goods, services and code travel between providers and customers. Complexity is so great that many organisations would be hard pressed to even name all of their suppliers. Yet as the pandemic highlighted, the uninterrupted flow of especially time-sensitive products is absolutely critical to economic stability and business growth.

Organisations are only as strong as their weakest supplier. So it's of some concern that two-thirds (64%) of respondents admit supply chain information security risks are becoming more common.

The challenge is that as supply chains become ever more reliant on IT systems, the opportunity grows for threat actors to target weak links. And organisations are only as strong as their weakest supplier. So it's of some concern that two-thirds (64%) of respondents admit supply chain information security risks are becoming more common. That figure rises to 70% in a tech sector dominated by complex digital supply chains. It is almost as concerning that just 29% of legal respondents say the same, considering law firms themselves are a significant target for threat actors given the wealth of sensitive client data they hold.

The vast majority (79%) of information security professionals we spoke to admit that theoretical risk has translated into at last one material supply chain security incident over the past 12 months. Nearly half (45%) say there have

TO WHAT EXTENT DO YOU AGREE OR DISAGREE WITH THE FOLLOWING STATEMENT:
THIRD-PARTY/SUPPLY CHAIN INFORMATION SECURITY RISKS ARE BECOMING MORE COMMON



Nearly half (45%) say there have been multiple incidents impacting their business, rising to over half of financial (53%) and retail (53%) sector respondents and 60% of those from the energy/utilities vertical.

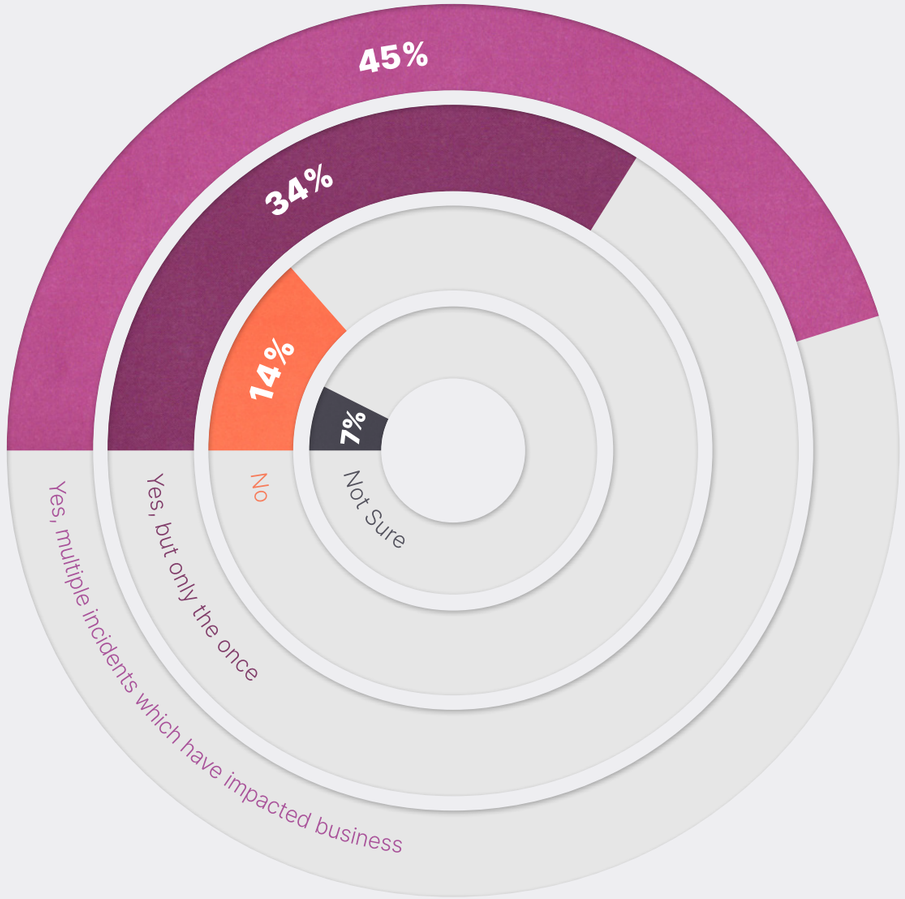
been multiple incidents impacting their business, rising to over half of financial (53%) and retail (53%) sector respondents and 60% of those from the energy/utilities vertical. It drops as low as 28% for education sector respondents, possibly as they have yet to discover breaches, rather than the fact the industry is less exposed to supply chain risk.

Third-party breaches can take many forms. Sometimes it is managed service providers (MSPs) and business process outsource (BPO) firms that are targeted because a breach at one of these companies could give the threat actor access to a large number of client networks or data. This was the rationale behind a 2021 ransomware attack on Latin American BPO giant Atento which the firm admitted cost over $40m.

At other times, a single supplier may be breached in order to gain a foothold in a high-target client. A 2022 ransomware breach at UK IT services firm Advanced had a catastrophic impact on NHS services. And increasingly, supply chain breaches take the form of attacks against a software developer or upstream open source project/repository.

A zero-day exploit targeting popular MOVEit file transfer software may have impacted over 1,000 corporate customers and as many as 60 million downstream individuals. A sophisticated multi-year attempt to backdoor popular open source component xz Utils was foiled by chance only at the last minute.

IN THE LAST 12 MONTHS, HAS YOUR BUSINESS BEEN IMPACTED BECAUSE OF A CYBER SECURITY/INFORMATION SECURITY INCIDENT CAUSED BY A THIRD-PARTY VENDOR OR SUPPLY CHAIN PARTNER?



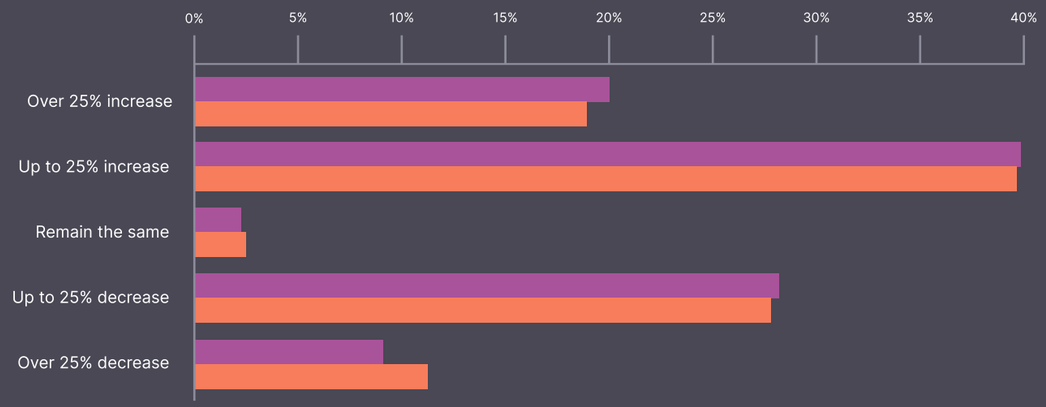
SECTORS CITING MANAGING VENDOR AND THIRD PARTY RISKS AS A CHALLENGE THEY ARE CURRENTLY FACING

52% TECHNOLOGY

50% EDUCATION

40% MANUFACTURING

HOW DO YOU EXPECT YOUR COMPANY'S INFORMATION SECURITY SPEND TO CHANGE IN THE NEXT 12 MONTHS, IN THE FOLLOWING AREAS?



08

HOW ORGANISATIONS ARE MANAGING SUPPLIER RISK

Managing these vendor and third party risks is the number one challenge of respondents we polled, cited by 38%. The figure rises to 50% of education sector respondents and 52% of those working in the technology space. On the one hand, it's good to see that more money is being allocated to such initiatives. Two-fifths (40%) of responding infosecurity professionals say allocations for securing supply chain and third-party vendor connections are set to increase by up to 25% in the coming year. And a further fifth (20%) claimed the increase would amount to more than 25%.

However, as in other areas, the devil will be in the detail. Zero trust approaches could help to mitigate the risks posed by supplier access to sensitive assets and resources. So it's reassuring to see 58% of respondents claim they're investing more in the next year on these initiatives. And that a fifth (40%) have adopted a zero trust model over the past 12 months. But zero trust won't necessarily help with the challenge of software supply chain security.

A fifth (40%) have adopted a zero trust model over the past 12 months. But zero trust won't necessarily help with the challenge of software supply chain security.

As we'll discuss, organisations are also increasingly requiring their suppliers to provide enhanced security assurance by demonstrating adherence to best practice certifications and standards. These include ISO 27001 for information security and ISO 27701 for privacy information management governance.

09

AI IS PART OF THE PROBLEM AND THE SOLUTION

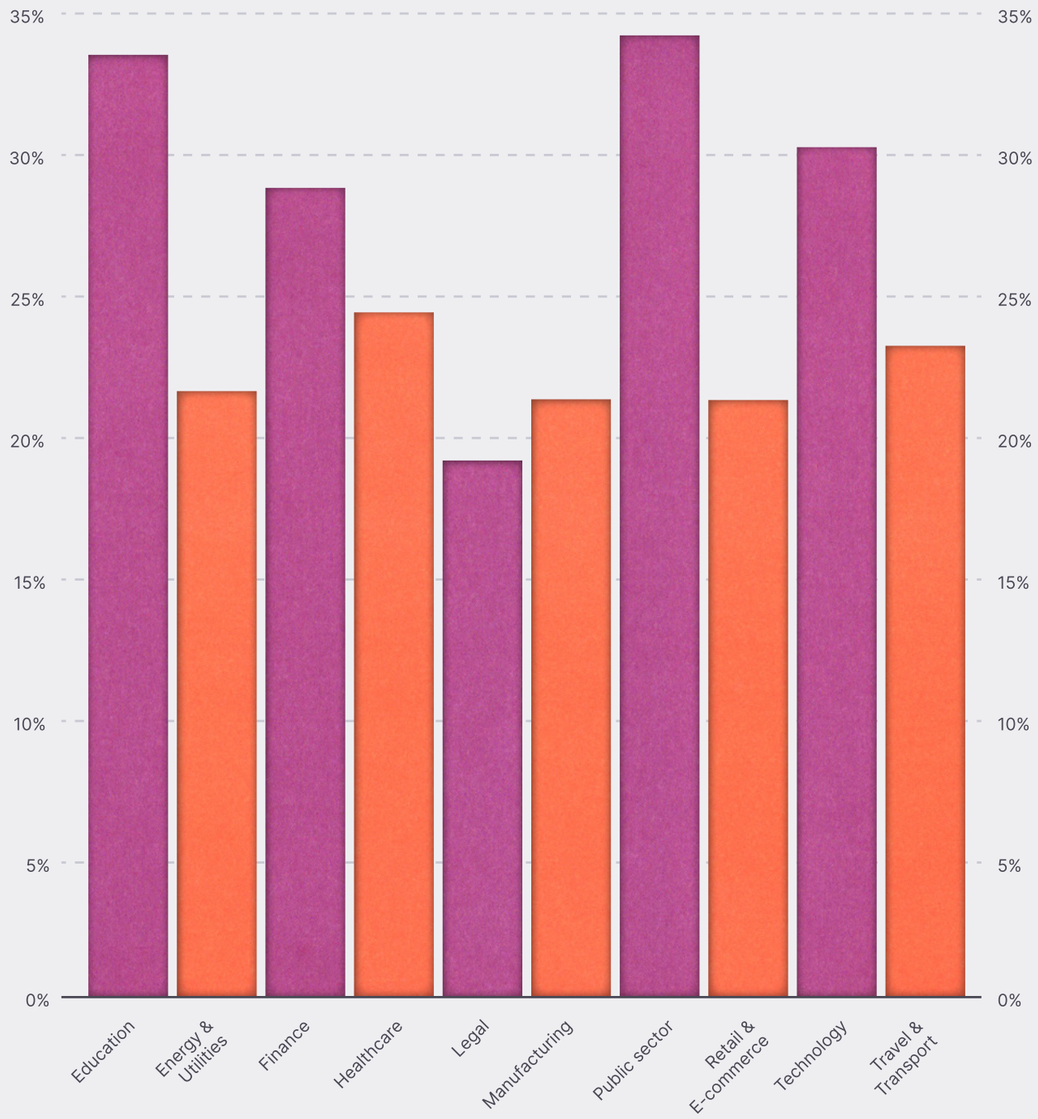
Generative AI (GenAI) may be the talk of boardrooms across the globe thanks to the breakout success of ChatGPT. But surprisingly just 26% of overall respondents say they adopted new technologies such as AI, machine learning (ML), and blockchain for security over the past year. It's particularly surprising given that AI uses for cybersecurity stretch way beyond GenAI. In fact, ML has been deployed for uses cases like spam filtering for many years. That said, the reticence of respondents to engage in new projects may explain why only 11% say that managing and securing emerging technology such as AI, ML and blockchain is among the biggest infosec challenge they're currently facing.

An even smaller share (7%) cite AI privacy breaches – an emerging concern of many organisations as they start to use GenAI in the workplace. Already, high-profile incidents are emerging of organisations that have unwittingly shared sensitive corporate or customer information via GenAI prompts. In tools like ChatGPT, this raises the risk that the information could be made available to other users outside the organisation. Samsung workers unwittingly shared internal meeting notes and source code in this way.

Already, high-profile incidents are emerging of organisations that have unwittingly shared sensitive corporate or customer information via GenAI prompts.

Analyst Forrester predicted that 2024 could see major data breaches and regulatory fines for corporate GenAI users – highlighting another threat; insecure code created by these tools. Warnings have also been issued by the UK's National Cyber Security Centre (NCSC), among others, that GenAI will exacerbate the ransomware threat, by making reconnaissance and social engineering easier. As

HAVE YOU ADOPTED NEW TECHNOLOGIES SUCH AS ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) AND BLOCKCHAIN FOR SECURITY IN THE LAST 12 MONTHS?



EXPECTED SPEND ON INVESTMENT IN AI AND ML SECURITY APPLICATIONS OVER THE NEXT 12 MONTHS

we've discussed, AI-powered deepfakes are already a significant challenge for respondents to this research.

Yet despite these ominous predictions, three-quarters (76%) of security professionals we asked in the US, UK and Australia actually believe AI and ML technology is improving information security. And an overwhelming majority (64%) are increasing their budgets accordingly over the coming year.

They're certainly right to explore the opportunities. GenAI alone is already being touted by security vendors as a way to bridge skills gaps in the Security Operations Centre (SOC), by explaining and contextualising alerts and complex scripts, and recommending response actions. If trained on the right datasets, it could also help teams to prioritise patches and identify common misconfigurations. The technology's ability to produce synthetic data may even be useful for simulating attacks in order to test AI/ML-powered security tools.

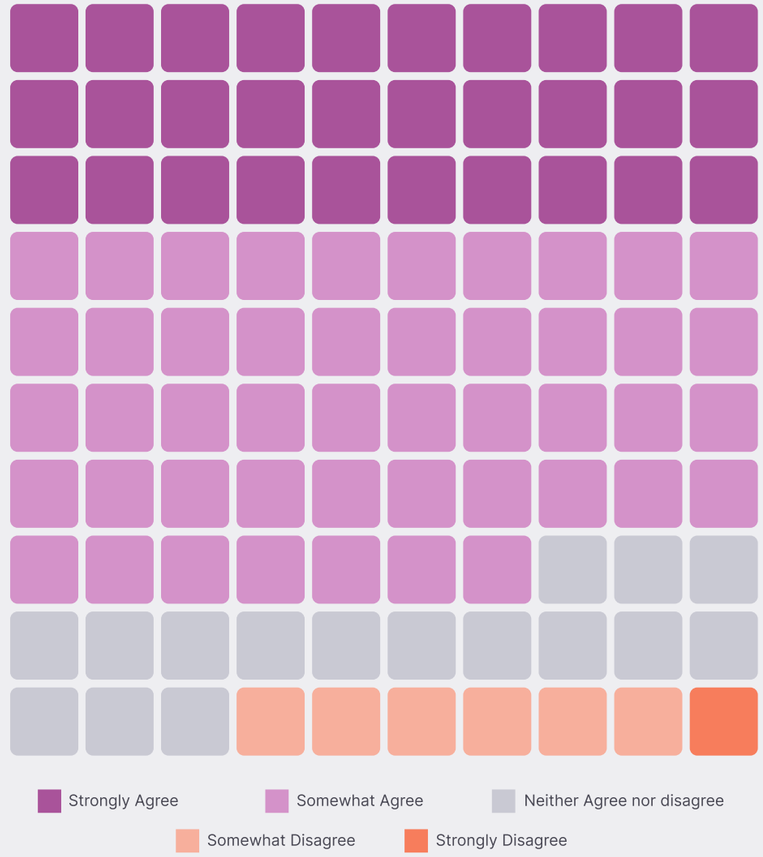
One thing is certain: the direction of travel at a government level is for more, not less regulation. The EU is undoubtedly leading the way here with its EU AI Act, which holds all AI providers, deployers, importers, distributors and product manufacturers accountable – and introduces conformity assessments for high-risk AI systems. The US has so far relied on Presidential executive order to set standards on security and privacy protections, with a possible federal law coming in time. And even the UK is now signalling its intent to regulate, having previously taken a hands-off approach.

One thing is certain: the direction of travel at a government level is for more, not less regulation.

Against this backdrop, standards like ISO 42001 will help organisations provide assurances to regulators. Although just 13% of our respondents are using information security and compliance to boost secure adoption of new technologies, this figure will surely rise as both technology use and regulatory action becomes more widespread.

Despite these ominous predictions, three-quarters (76%) of security professionals we asked actually believe AI and ML technology is improving information security.

TO WHAT EXTENT TO YOU AGREE WITH THE FOLLOWING: ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING TECHNOLOGY IS IMPROVING INFORMATION SECURITY



10

COMPLIANCE DRIVES A RANGE OF BUSINESS BENEFITS

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 (UK RESPONDENTS)

Compliance has historically often been viewed by boardrooms as a necessary evil: a means to avoid punitive fines and bad publicity. But our research reveals that things are changing. On the ones hand more UK respondents are being fined between £250-500K (26% today versus 21% in 2023). And a lot more are being fined £100K-250K (35% vs 18%).*(no comparatives are available for the US and Australia).

Yet fines are only one part of the compliance story. Only 19% of respondents say their main motivation for compliance is to avoid penalties. Far more talk about remaining competitive (34%), increasing customer demand (34%), and protecting business (30%) and customer (29%) information. A sizeable share (27%) are also motivated to deliver strong compliance programmes by the prospect of entering new markets and supply chains.

All of the above is certainly true. But there are even more potential benefits. In fact, respondents report that their biggest return on investing in compliance programmes over the past year has been enhancing their business reputation as a secure and reliable entity (34%). They also cite direct cost savings from a reduced number of cybersecurity incidents (30%), time savings from more efficient security processes (29%) and greater appeal to investors looking for low risk companies (28%). A significant share also say they've streamlined security infrastructure so it is easier and less costly to manage (28%) and that they've driven significant ROI from compliance by improving the quality of business decisions due to secure and reliable data (26%). Only a fifth (19%) say the same about avoiding fines and penalties.

Standards and certifications can help to deliver the foundation on which strong regulatory compliance programmes can be built. They are especially important when one considers that 65% of respondents find the rapid pace of regulatory change is making it harder to comply with information security best practices. So where are UK, US and Australian organisations focusing their efforts? The most popular standard is ISO 9001 for quality management (25%), followed by ISO 27001 for information security (23%) and ISO 27701 for privacy information management (22%).

It's encouraging to see such widespread take up of these standards. In fact, 59% of respondents say they're planning to increase spending on these programmes over the coming year, with a fifth (19%) ramping up investment by over 25%. Yet challenges persist. Nearly half (46%) of respondents say it takes them between six and 12 months to comply with ISO 27001. A further 11% say it takes between 12 and 18 months, while 5% claim it takes more than a year-and-a-half.

It doesn't have to be this way. Organisations need trusted compliance partners to help streamline the process.

11

HOW HAS THE UK SECURITY LANDSCAPE CHANGED?

Phishing attacks, data breaches, and malware infections were the top security incidents in 2023. Although malware and social engineering point to a similar top three in 2024, this year also saw deepfakes making an appearance for the first time. Threats are becoming all pervasive. The share of respondents who haven't been a victim of a cyber-attack fell from 9% to 0% over the period.

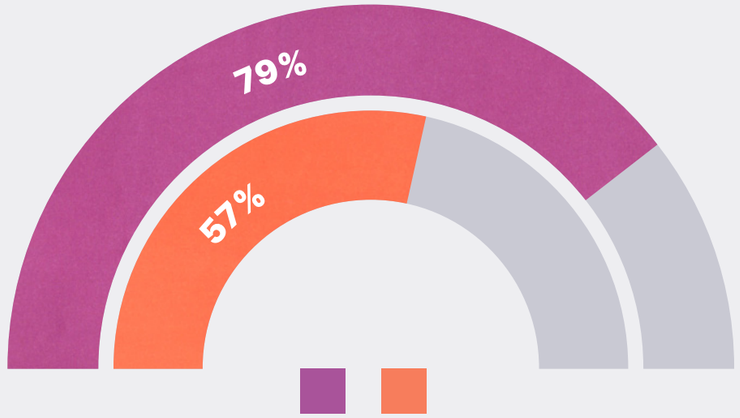
However, more positively, those experiencing a data breach decreased from 36% to 23%. Half (50%) of respondents last year listed financial data as most at risk of being compromised. Now it's partner data (41%) in first place, followed by financial information (38%).

Virtually all (98%) organisations last year claimed they face information security challenges in their attempts to improve security, with budget constraints as the top challenge. Now every single respondent (100%) is facing challenges, but the most common is managing vendor and third-party risk (38%). That's an increase from 30% last year. Another stat hints at why: in 2023, just 57% of companies said they'd suffered at least one information security incident due to their supply chain in the previous 12 months. By 2024 this number had soared to 79%.

In 2023, the second and third-placed challenges were human-centric, with the skills gap coming in second (36%) followed by insider threats (33%). This year, these were replaced by compliance and skills gaps (both 32%). Last on the list of 10 challenges last year was managing Bring Your Own Device (BYOD) security (25%). By 2024, it had risen again to fourth (30%) – an indication that the threat landscape is in constant flux and risk must be continually managed.

100%

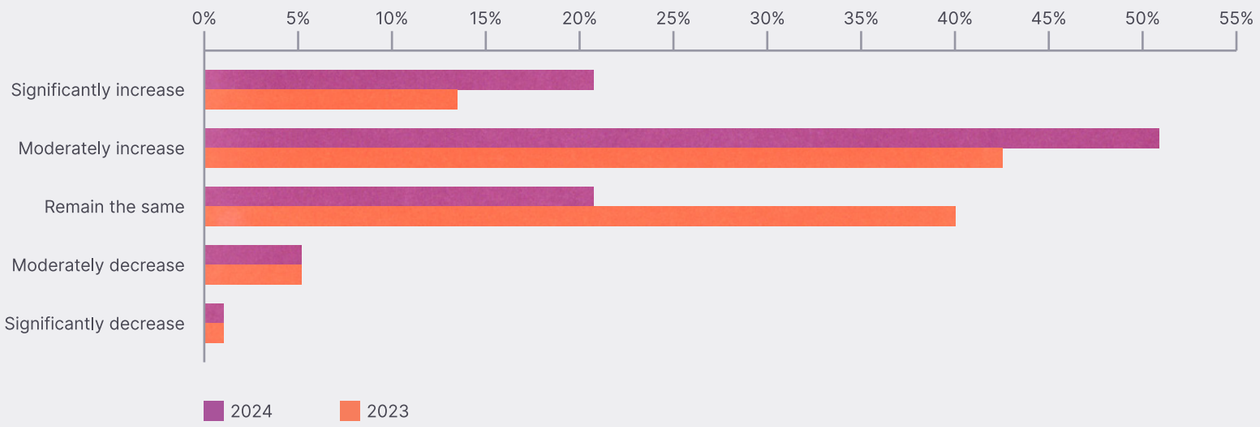
VICTIMS OF CYBER ATTACK ROSE FROM 91% (2023) TO 100% (2024)

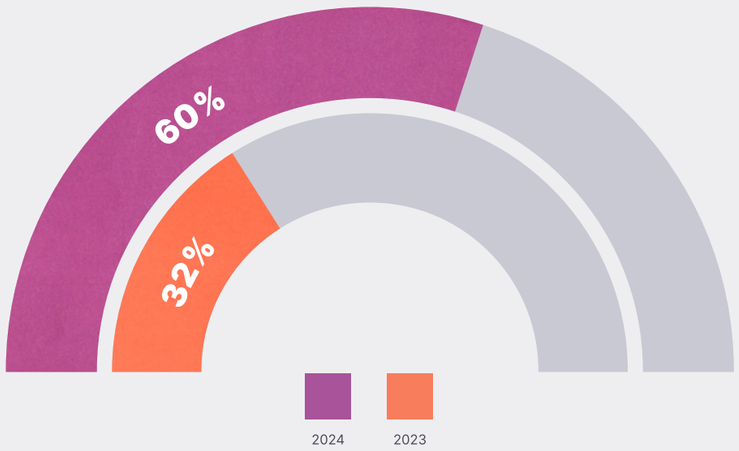


IN 2023 57% OF COMPANIES SAID THEY'D SUFFERED AT LEAST ONE INFORMATION SECURITY INCIDENT DUE TO THEIR SUPPLY CHAIN IN THE PREVIOUS 12 MONTHS. BY 2024 THIS NUMBER HAD SOARED TO 79%.

TOP CHALLENGES FACED BY BUSINESSES

SPEND ON OVERALL INFORMATION SECURITY INITIATIVES AND RESOURCES OVER THE NEXT 12 MONTHS VS PROJECTED 2023





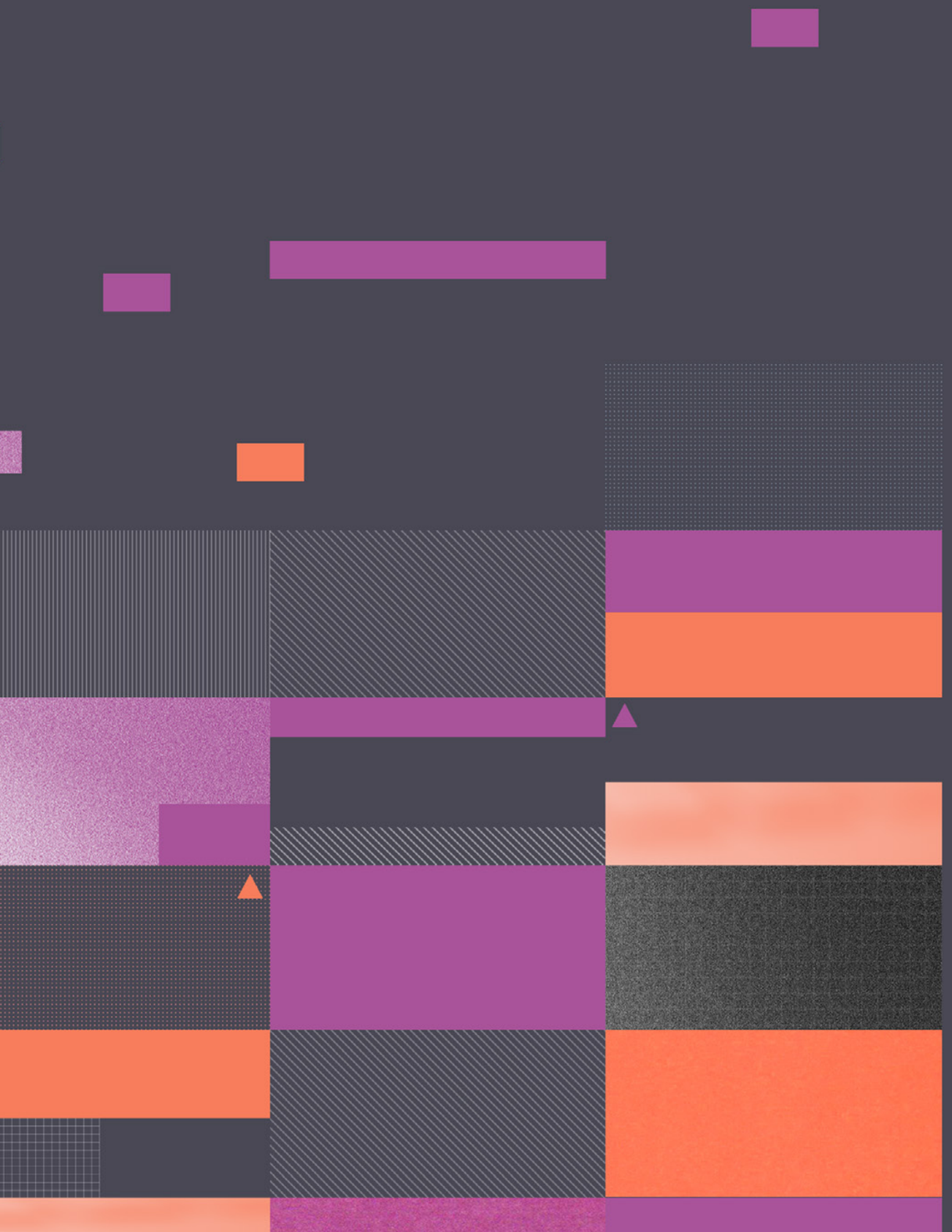
THE SHARE OF RESPONDENTS WHO THINK THAT SENIOR LEADERS IN THEIR BUSINESS VIEW STRONG INFORMATION SECURITY AS A TOP PRIORITY INCREASED FROM 32% TO 60% OVER THE PERIOD

59% complained about the rapid pace of regulatory change, yet only 64% said they have a clear information security policy in place – a concerning trend if it persists next year

When it comes to compliance programmes, nearly 7 in 10 (69%) professionals claimed last year that the blistering pace of change makes it harder to comply with infosec regulations. This was despite the fact that 80% stated that they have a clear information security policy in place. A year later, just 59% complained about the rapid pace of regulatory change, yet only 64% said they have a clear information security policy in place – a concerning trend if it persists next year.

The share of companies who admit they're struggling with regulatory compliance rose from 27% last year to 32% in 2024. However, more welcome is the news that the mean length of time it takes to comply with ISO 27001 decreased from 15.5 months to 8.8 months over the period. It can go lower still with the right technology tools and partner.

Ending on an optimistic note, the share of respondents who think that senior leaders in their business view strong information security as a top priority increased from 32% to 60% over the period. That could be reflected in the number reporting an increase in budgets. In 2023, 35% said their overall infosec budgets would stay the same, and 45% stated that their infosec teams would not grow over the next 12 months. Now 72% claim their budgets are increasing and 60% that their teams will grow.



The bottom line is that compliance doesn't need to be as onerous as businesses might think. Help is at hand.

12

CONCLUSION

IT and business leaders across the UK, US, Australia and beyond are battling the same challenges. Digital transformation is essential to drive competitive advantage and improve process efficiencies. Yet these same investments in cloud, AI, IoT and other projects are at the same time expanding the digital attack surface. Faced with agile, determined and resourceful adversaries, organisations are struggling to keep data secure, services operational and regulators happy. These challenges will only worsen as the attack surface grows and regulators become less forgiving.

Against this backdrop, compliance with best practice frameworks and standards offers hope. They can provide the foundational processes businesses need to deliver critical assurances to customers, shareholders and regulators. That's why take-up continues to grow across the globe – whether it's NIST, ISO, Cyber Essentials, or other frameworks and standards. Yet rising regulatory fines prove there's still some way to go. The bottom line is that compliance doesn't need to be as onerous as businesses might think. Help is at hand.

SAM PETERS
CHIEF PRODUCT OFFICER, ISMS.ONLINE

INFORMATION SECURITY DRIVING BUSINESS EXCELLENCE

The ISMS.online and Censuswide report underscores the importance of information security and compliance today. As organisations embrace digital transformation, they encounter growing cyber threats. Exceptional information security, data privacy, and cybersecurity standards are now essential for business success.

At ISMS.online, we understand organisations' challenges in navigating this complex landscape. Our all-in-one compliance platform is designed to empower businesses to achieve simple, sustainable security that scales with their growth. Built on the globally recognised ISO 27001 framework, our platform helps organisations identify, assess, and prioritise information security risks, implement effective controls, and ensure ongoing monitoring and review.

The report underscores the importance of investing in employee cybersecurity awareness and training programs and the potential of AI and ML technologies to enhance information security. We remain committed to incorporating these insights into our platform, empowering our clients with the tools and expertise they need to harness the power of these technologies while maintaining compliance with the latest regulations and standards.

Our user-friendly platform comes preconfigured to help businesses achieve over 80% compliance with ISO 27001 and accommodates more than 100 other regulations, industry standards, and laws, including GDPR, ISO 27701, ISO 42001, NIST, and HIPAA.

By streamlining compliance processes, providing real-time insights, and facilitating collaboration across teams, we enable organisations to unlock the multifaceted benefits of robust compliance programs, from enhanced reputation to improved decision-making.

As the cyber risk landscape evolves, organisations prioritising information security and compliance will set themselves apart and unlock their growth potential.

As the cyber risk landscape evolves, organisations prioritising information security and compliance will set themselves apart and unlock their growth potential. At ISMS.online, we stand ready to support businesses on this critical journey, driving innovation and thought leadership to help our clients stay ahead of the curve. With our platform as a foundation, organisations can achieve the simple, sustainable security they need to thrive in the digital age.

ABOUT ISMS.ONLINE

ISMS.online is revolutionising the way businesses across the globe handle data privacy and information security compliance.

The cutting-edge SaaS platform provides a comprehensive roadmap to robust and scalable governance, risk and compliance for organisations of all sizes and maturities.

With a global presence and over 25,000 users, including enterprise clients like Moneycorp, Siemens and Ricoh, ISMS.online simplifies complex processes across over 100 standards and regulations, empowering organisations worldwide to secure and scale their compliance with ease.

isms.online