THE STATE OF INFORMATION SECURITY REPORT 2023

HOW SMART BUSINESSES ARE UNLOCKING THE POTENTIAL OF STRONG INFORMATION SECURITY

isms.online

PUBLIC V1.0

CONTENTS

The ISMS.online report provides detailed insight into the current information security landscape and identifies how organisations can build cybersecurity programs that leverage people, processes and technology to drive business success.

EXECUTIVE SUMMARY

PEOPLE, PROCESSES AND TECHNOLOGY: THE COMPLIANCE ADVANTAGE

With new technologies emerging and cyber criminals becoming increasingly sophisticated, businesses can no longer view information security as a tick-box exercise.

Instead, they should take a proactive approach to ensure that their information systems are robust enough to withstand the sophisticated risks of the expanding threat landscape.

Hybrid work models, expansive IT networks, increased use of Internet of Things (IoT) solutions and the sudden acceleration in AI necessitate intensified approaches to information security. Adding to the complexity are numerous regulations that are enacted and updated at an ever-increasing rate.

Staying ahead of cyber risks can be challenging, but our research indicates that organisations that build digital trust by investing in their information security can unlock two key benefits. Firstly, they are much less likely to fall victim to a cyber-attack or data breach, meaning they can avoid costly financial and reputational damage. Secondly, they establish themselves as trustworthy and reliable partners in the digital space, allowing them to grow faster and more securely than their competitors.

The prominence of human-centric challenges indicates that information security is as much a people issue as a tech issue.

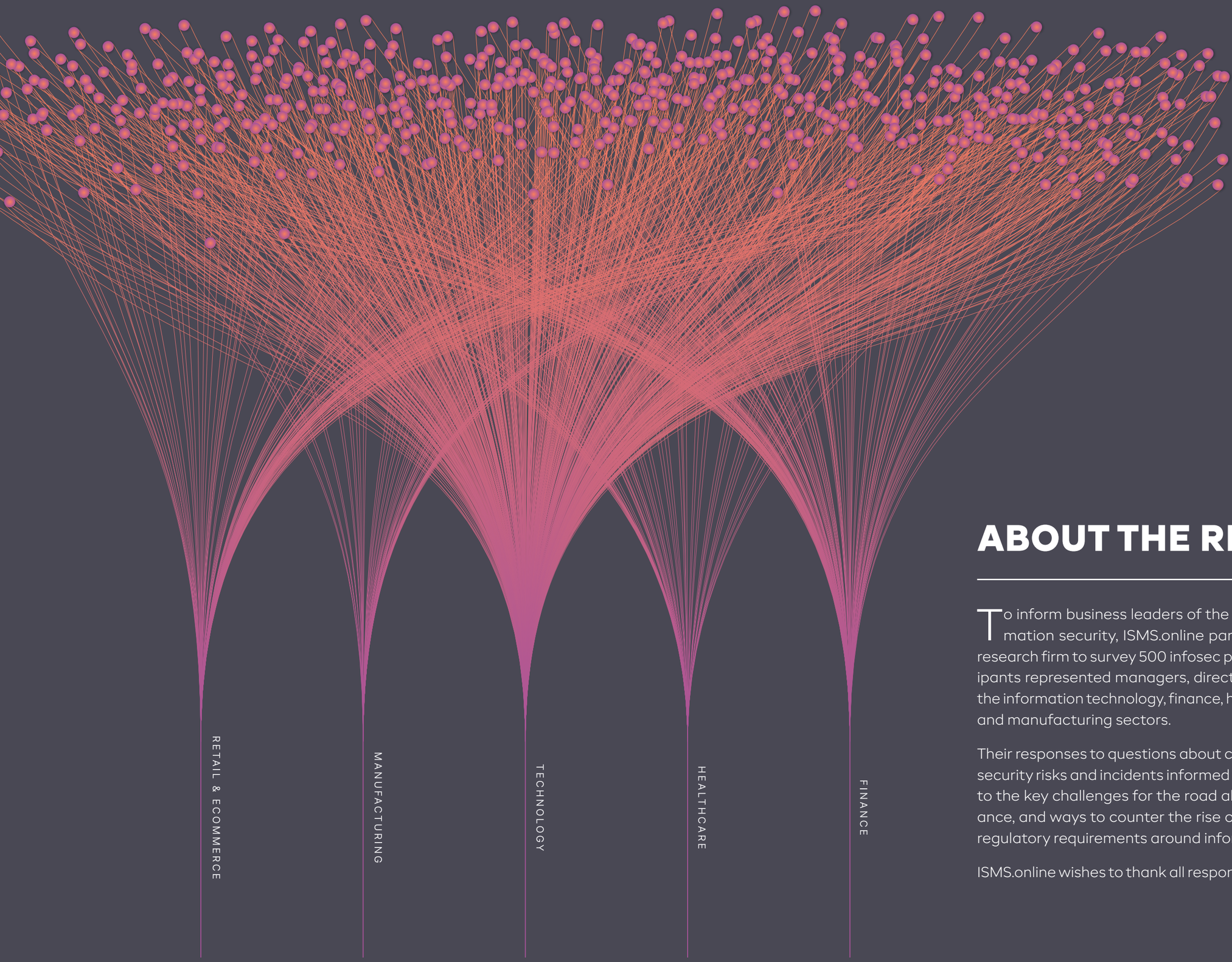
This explains why almost half the respondents (46%) listed the growth of digital trust mechanisms as a top information security opportunity. At the other end of the scale, those decreasing their information security budgets and internal team size suffered the most penalties for data breaches and regulatory violations.

As reflected in this report, the prominence of human-centric challenges indicates that information security is as much a people issue as a tech issue. The people aspect includes a skills shortage at a technical level and the risk of senior executives making inadequate critical decisions around strategy and budgets.

Many younger people (those aged 25-34) entering the sector seem to push the 'never trust, always authenticate' envelope more than their older counterparts, who seem less concerned about zero-trust security models. This could signify that the next generation of CISOs will view the zero-trust model as essential.

Calls for more global harmony in information and data privacy regulations are also growing louder, since greater consistency in standards would significantly reduce compliance challenges. Having ISO 27001 and other relevant certifications enables companies to cover both the regulatory requirements and industry standards while continuously monitoring and improving risk assessment and threat intelligence.

Information and cyber security touch many areas and vary significantly from company to company. No single set of best practices can cover every situation, but good practice increasingly provides a competitive advantage. Implementing the necessary standards and controls today will help set your business up for secure, sustainable success in the long term.

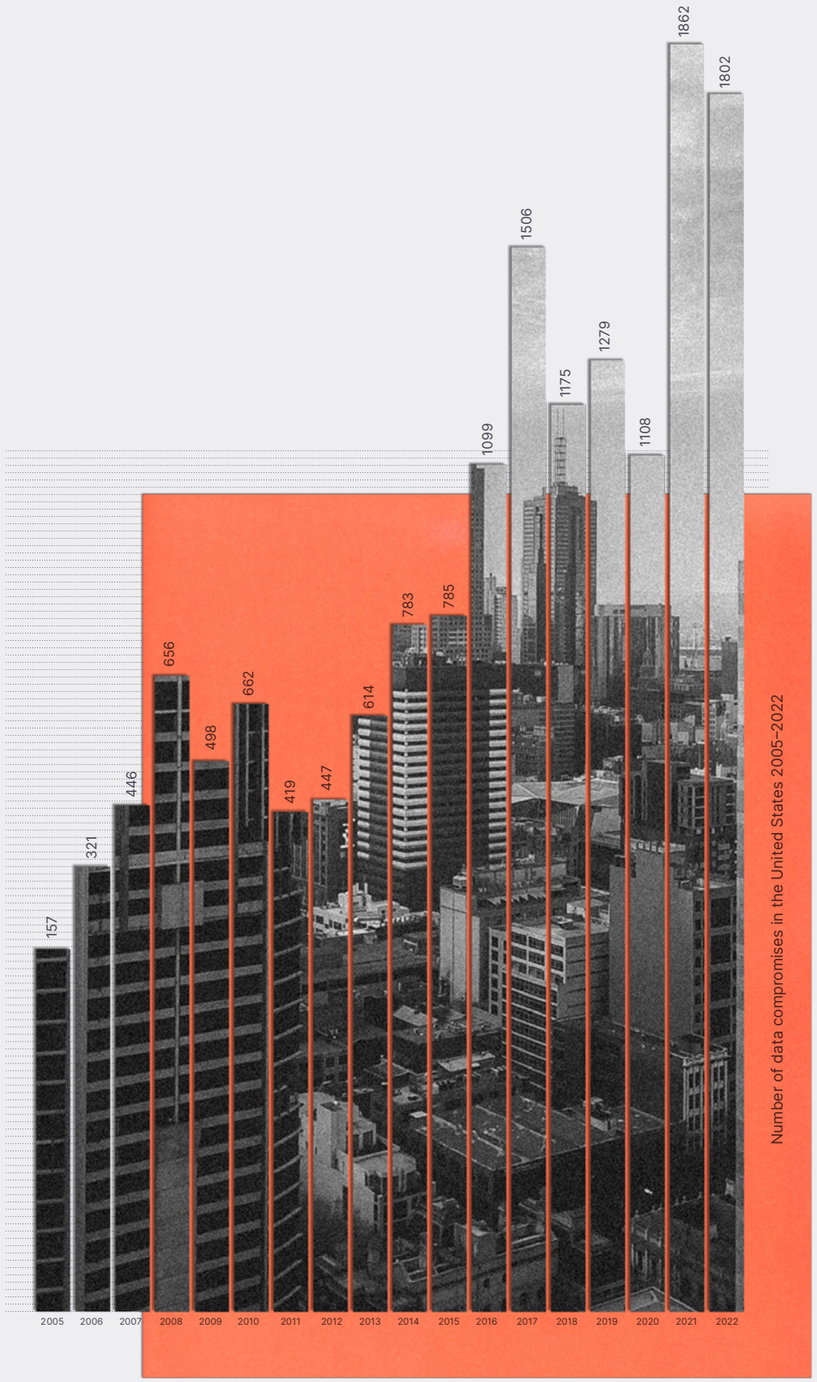


ABOUT THE RESEARCH

To inform business leaders of the current state of play in information security, ISMS.online partnered with an independent research firm to survey 500 infosec professionals in the UK. Participants represented managers, directors and C-level executives in the information technology, finance, healthcare, retail, e-commerce and manufacturing sectors.

Their responses to questions about cybersecurity and information security risks and incidents informed this report. It draws attention to the key challenges for the road ahead, the benefits of compliance, and ways to counter the rise of cyberthreats and meet the regulatory requirements around information security.

ISMS.online wishes to thank all respondents for their valuable input.



Source: ITRC 2022 Annual Data Breach Report

THE INFORMATION SECURITY LANDSCAPE AND THE RISE OF THREATS

Today virtually every company, irrespective of size, is a data company.

Forward-thinking business leaders are leveraging the benefits of solid information security and privacy foundations, to build companies of the future that can withstand an ever-changing array of complex digital threats.

As businesses continue investing in technology and adding more systems to their IT networks to improve customer experiences, facilitate remote work and create value, cyber adversaries increasingly leverage more sophisticated methods and tools to compromise these systems. The risk is increased further by the proliferation of sensitive financial, customer and employee data that companies hold.

Gone are the days of lone hackers, with organised entities now employing integrated tools and capabilities, including artificial intelligence and machine learning. Small and mid-size enterprises and governments now face the same cyber risks as large corporations. As a result, the scope of threats organisations must tackle expand exponentially, and no organisation is immune.

Businesses that make themselves guilty of poor data management can incur high reputational and financial costs.

Businesses that make themselves guilty of poor data management can incur high reputational and financial costs. In severe cases, board members could even be held personally liable, and the damage to a business can be irreparable.

These risks, while real and significant, are not inevitable. Businesses must adopt a proactive and forward-thinking approach to mitigate this growing threat landscape.

Small and mid-size enterprises and governments now face the same cyber risks as large corporations.

SECTORS AND COMPANIES AFFECTED BY SECURITY INCIDENTS

Phishing attacks, data breaches, and malware infections are the top security incidents infosec professionals see within their businesses. According to the survey, more than one in three companies (36%) have had a data breach in the last 12 months. Such breaches are a top concern for the healthcare and financial services sector.

According to the survey, more than one in three companies (36%) have had a data breach in the last 12 months.

Notably, the data suggests that just nine per cent of respondents haven't been victims of a cyberattack, with the overwhelming majority (91%) having experienced at least one attack. The data also indicates that companies which reduce the size of their infosec teams are more exposed to phishing attacks and data breaches, even if they retain the same budget.

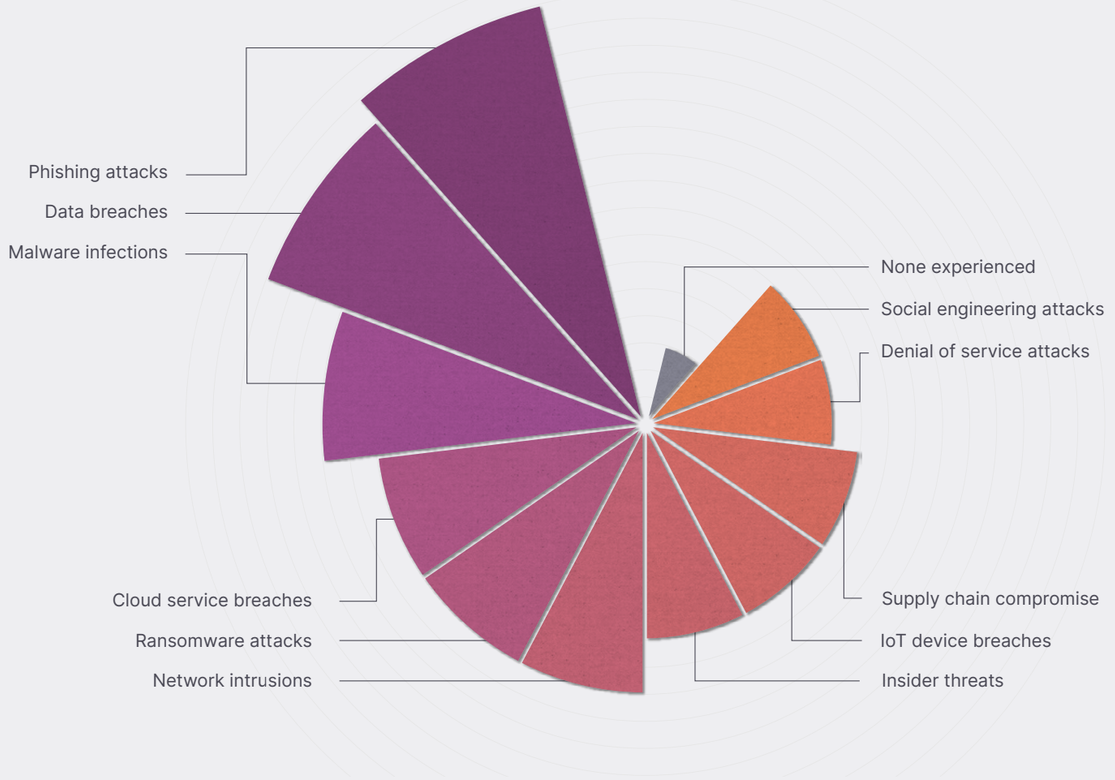
Those businesses increasing their budgets were often victims of previous cyberattacks, and it may well be they are strengthening budgets in response. The same applies to companies hit by supply chain cyberattacks, who often increase the budget and team size to prevent a repeat.

Unsurprisingly, 98% of respondents face information security challenges in their attempts to improve security, with budget constraints as the top challenge. This response may result from the current economic backdrop and tightening budgets.

As expected, CISOs with declining budgets and team sizes agreed their business leaders were less likely to take infosec seriously. Yet this seems not only limited to this group: 60% of respondents feel solid information security is only somewhat important to their senior leaders. This implies that many companies are unaware of the financial benefits, enhanced reputation, and operational efficiencies that good infosec brings.

Just nine per cent of respondents haven't been victims of a cyberattack, with the overwhelming majority (91%) having experienced at least one attack.

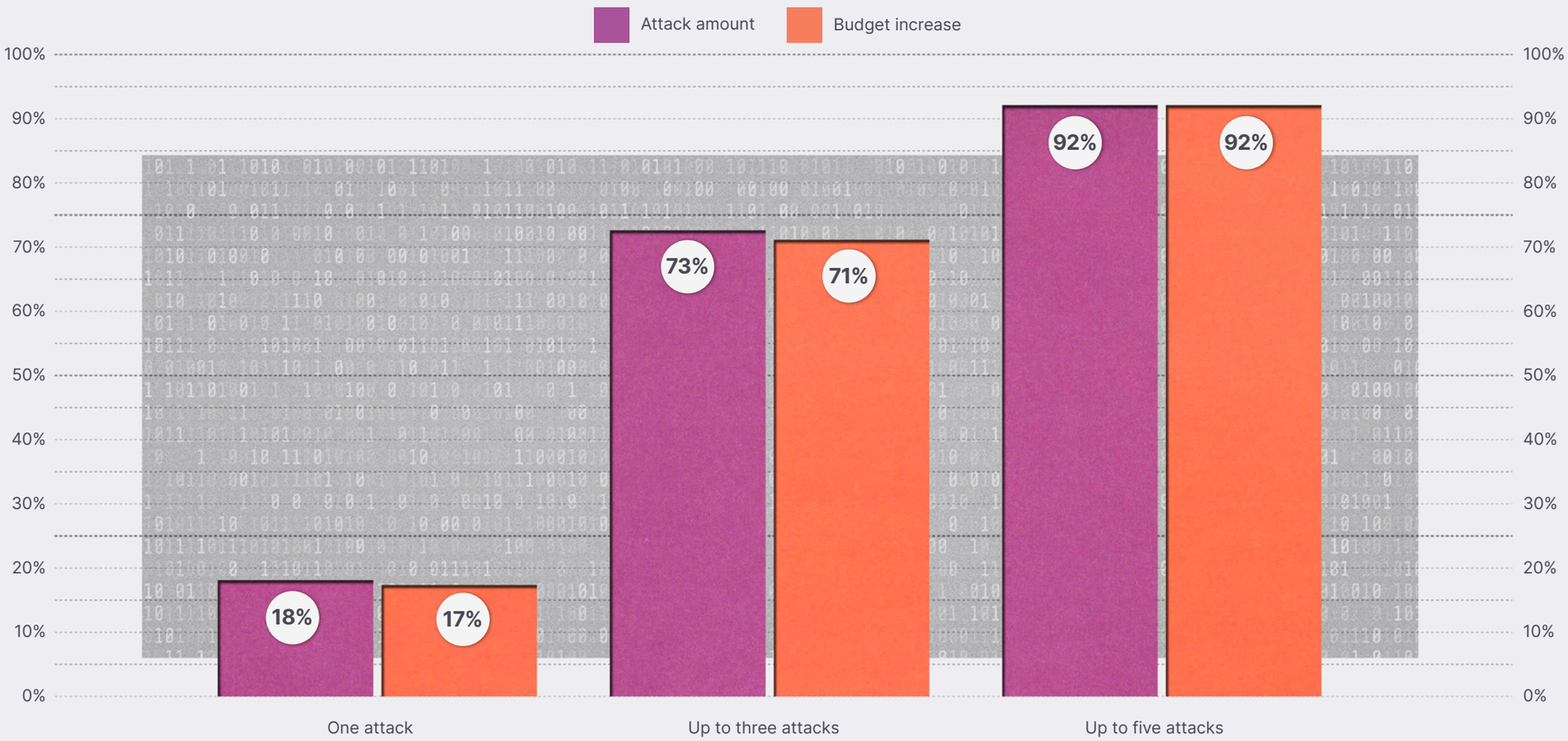
TYPES OF INCIDENTS EXPERIENCED IN THE PAST 12 MONTHS



MORE BREACHES, MORE HEFTY INFOSEC BUDGET INCREASES

Investing early to create a robust information security capability baseline will reduce the need for reactionary spending post-cyber incident(s) and ultimately mean lower infosec costs in the long term.

ATTACK BY VOLUME AND INFOSEC BUDGET INCREASES



INFRINGEMENTS HURT THE BOTTOM LINE

In the last 12 months, nearly two-thirds (60%) of UK businesses have received a fine due to data breaches or regulatory violations. The average total paid in fines was almost £250,000.

The most common fines for data breaches ranged from £50,000 and £100,000 (21%), followed by £100,000 to £250,000 (17.5%). Almost 21% of respondents received fines in excess of £250,000, with just under half admitting to receiving a fine ranging from £500,000 to a staggering £1,000,000.

Given the plethora of fines incurred, plus the intangible reputational damage that comes with a data breach, it makes more financial sense for companies to maintain close control of their infosec. In fact, investing in information security before being the victim of a cyberattack places a company in a much stronger position and saves money in the long term.

According to the Information Commissioner's Office (ICO), the UK's data protection regulator, a company's information security measures must be appropriate to the size and use of its network and information systems.

If a data breach occurs, the ICO will look at a company's information security setup when determining any fines it may issue.

It is important to note that if a data breach occurs, the ICO will look at a company's information security setup when determining any fines it may issue.

The high incidence of fines awarded is also an indication that many companies are not as effective at mitigating digital risks and achieving compliance with data standards as they would like to believe.

Investing in information security before being the victim of a cyberattack places a company in a much stronger position and saves money in the long term.

FINES RECEIVED BY AMOUNT

60%

OF ORGANISATIONS HAVE RECEIVED A FINE

£250,000

AVERAGE FINE RECEIVED

19%

HAVE RECEIVED A FINE OF £250,000 TO £1,000,000

FINES RECEIVED BY SECTOR

SENSITIVE DATA TARGETS

Half (49.9%) of the respondents listed financial data as most at risk of being compromised, which isn't surprising since financial services organisations safeguard vast volumes of sensitive information. One accidental click on a phishing email could give attackers access to thousands or even millions of customer records. Customer data came a close second at 48%, while 42% listed employee data as a risk factor.

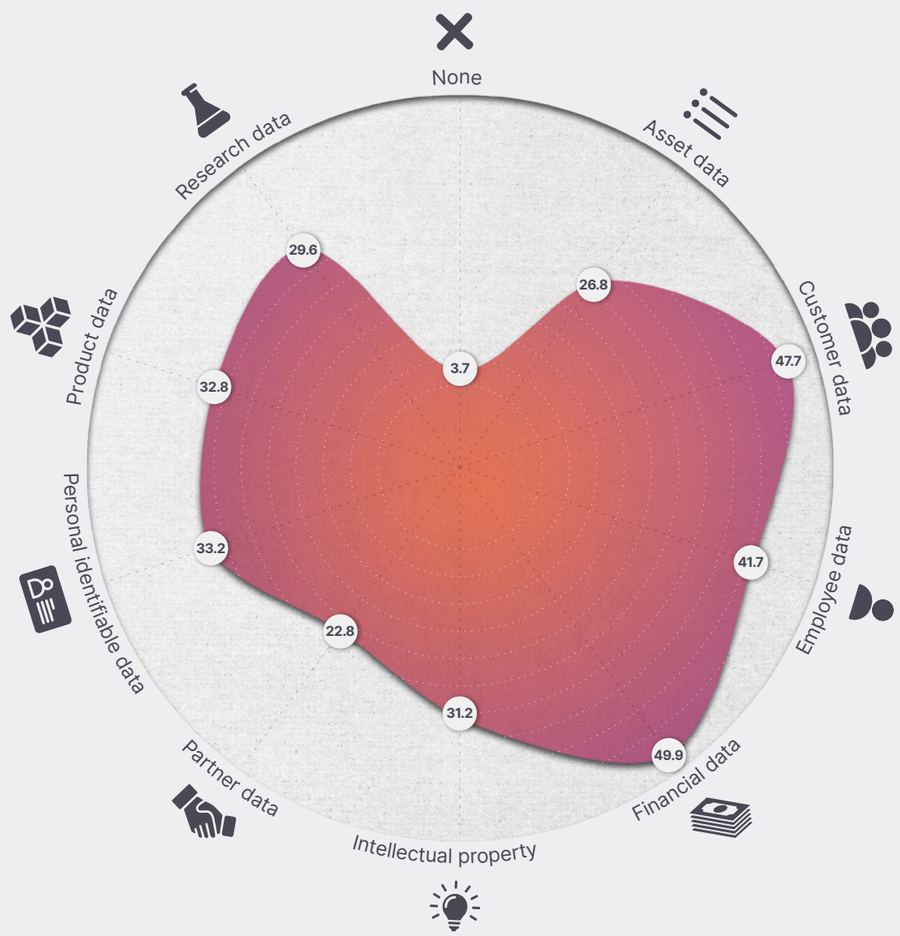
More than a third (39%) of survey respondents listed budget constraints as the top challenge in information security. Yet, the survey results show that those companies decreasing their budgets and team size suffered the most penalties. Perhaps unsurprisingly, it also took these companies noticeably longer to attain compliance with standards, including GDPR and ISO 27001.

TOP RESPONSES BY SECTOR

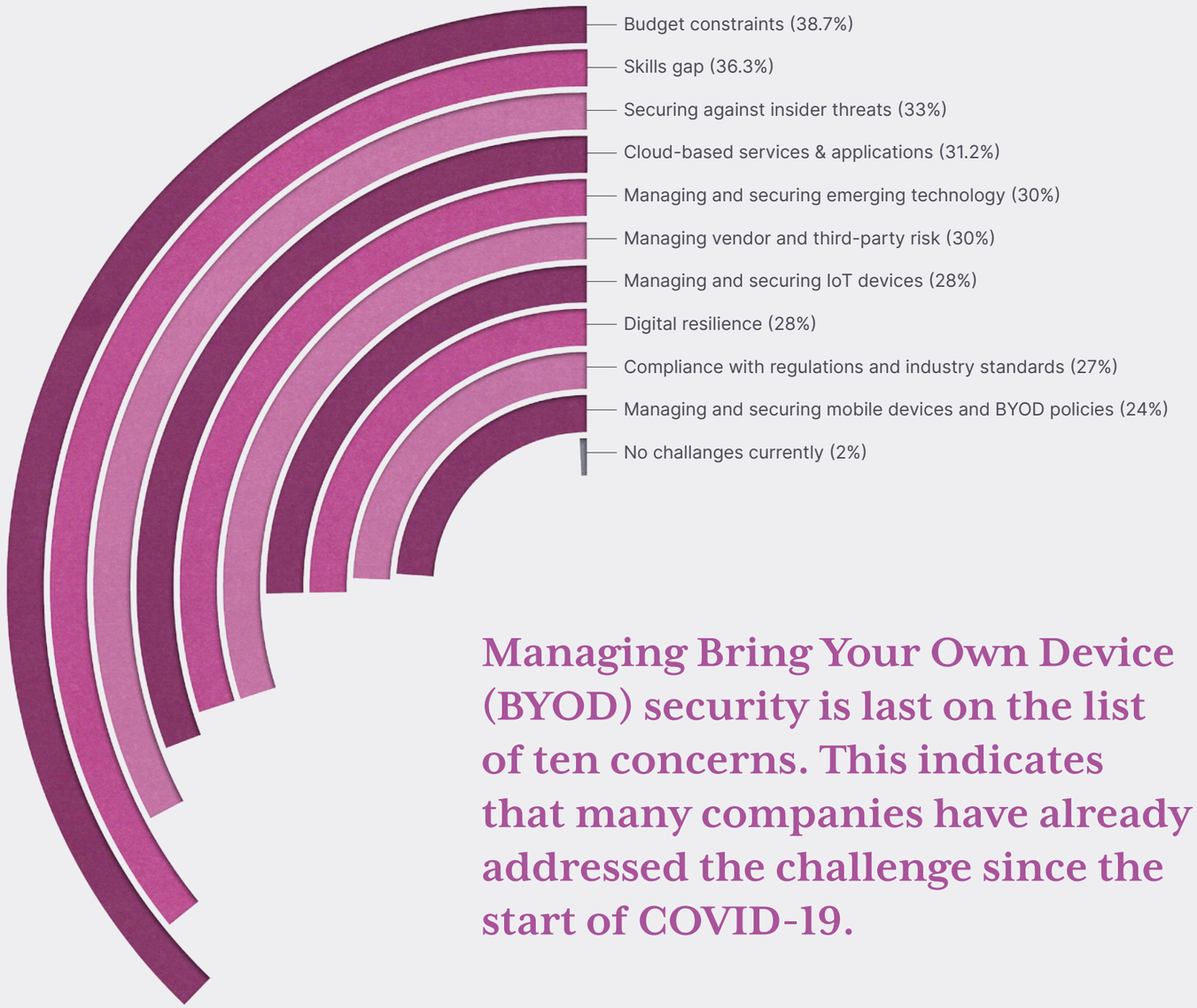
Finance			
Healthcare			
Manufacturing			
Retail			
Technology			

One accidental click on a phishing email could give attackers access to thousands or even millions of customer records.

WHAT TYPES OF DATA ARE MOST AT RISK OF COMPROMISE IN YOUR BUSINESS?
(TOTAL RESPONSE PERCENTAGES)



CURRENT INFORMATION SECURITY CHALLENGES FACED BY ORGANISATIONS



Managing Bring Your Own Device (BYOD) security is last on the list of ten concerns. This indicates that many companies have already addressed the challenge since the start of COVID-19.

The following two challenges are human-centric, with the skills gap coming in second at 36%, followed by securing against insider threats (33%). This indicates that information security is as much a people issue as a tech issue.

The survey results show that those companies decreasing their budgets and team size suffered the most penalties. Perhaps unsurprisingly, it also took these companies noticeably longer to attain compliance with standards, including GDPR and ISO 27001.

Each challenge affects at least a quarter (25%) of infosec professionals, so the range of issues is broad. Managing supply chain risk (30%) is also a considerable difficulty, especially given the recent spike in cyber threats. Businesses often collaborate closely with suppliers and resellers, so computer networks may become intertwined or share sensitive data. If one organisation gets breached, it can have serious knock-on effects.

Another noteworthy observation is that managing Bring Your Own Device (BYOD) security is last on the list of ten concerns. This indicates that many companies have already addressed the challenge since the start of COVID-19. The three years of hybrid working have increased the likelihood of employees using their personal devices for work. Employers have had to move quickly to prevent this from becoming a potential route to a breach.

Nearly three-quarters agree that information security is impossible without data privacy.

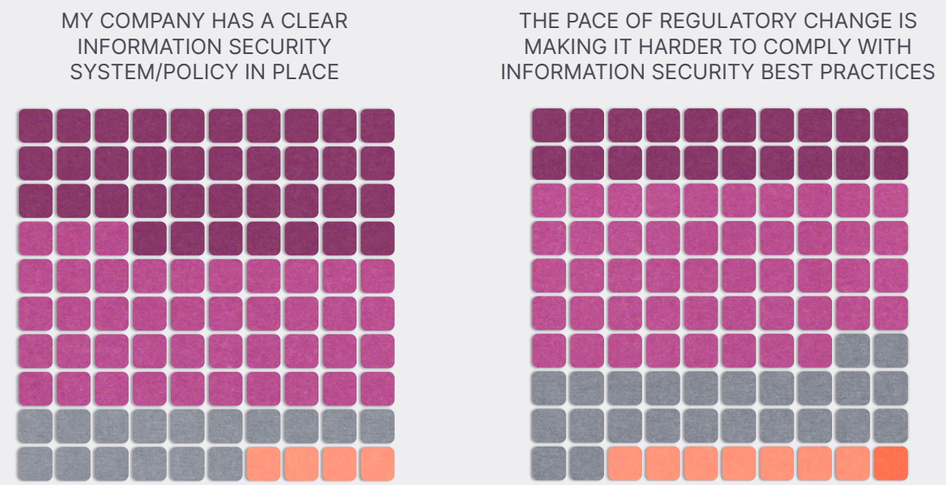
A MORE SOPHISTICATED THREAT LANDSCAPE

Regulators and legislators must constantly update approaches and best practices to keep up with the ever-changing information and cyber security landscape. However, nearly 7 in 10 (69%) professionals believe the blistering pace of change makes it harder to comply with infosec regulations. This is despite most (80%) believing they already have a clear information security policy in place.

Nearly 7 in 10 professionals believe the blistering pace of change makes it harder to comply with infosec regulations.

No wonder the vast majority (80%) of respondents favour more harmony in infosec regulations for information and data privacy, such as adopting a globalised standard like ISO 27001. Nearly three-quarters (73%) also agree that information security is impossible without data privacy.

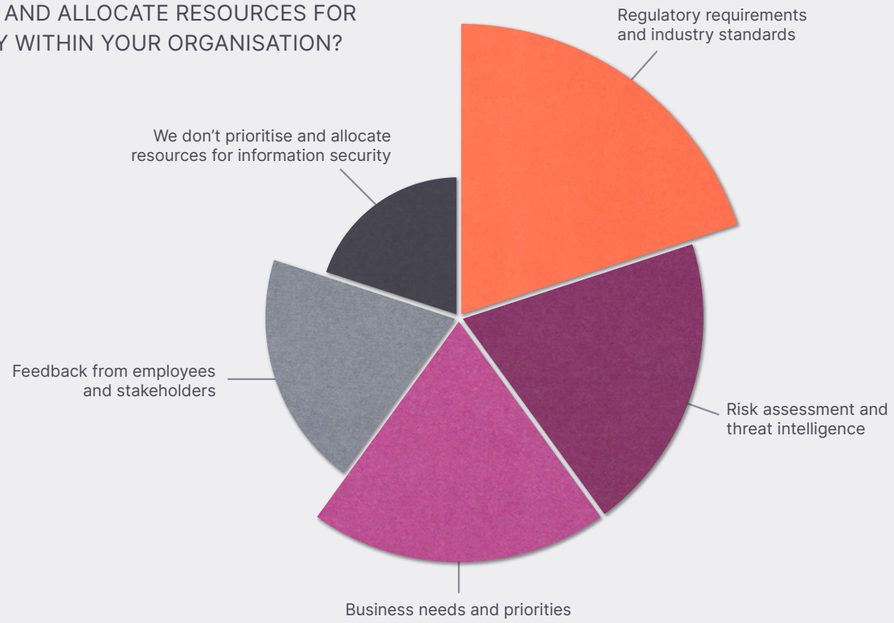
Migration to the cloud is an inevitable evolution of data storage and management, analytics, and reporting, making the threat landscape ever more sophisticated. Keeping tabs on these is a formidable challenge for those in information security, with over a quarter (28%) of companies investing more budget on cloud security over the next 12 months.



More than half (52%) of infosec professionals prioritise and allocate resources for information security within their organisations based on regulatory requirements and industry standards. Evenly split are those basing it on risk assessment and threat intelligence, and business needs and priorities. This is where an information security management system (ISMS) is invaluable since it would enable companies to address all three approaches.

Information security is challenging to measure, yet businesses must continuously evaluate its effectiveness – identifying potential weaknesses, vulnerabilities, and compliance issues. Over a third of respondents (40%) use the number of incidents and breaches as a measurement tool, followed by reduced security incidents and the time to detect and respond to breaches.

HOW DO YOU PRIORITISE AND ALLOCATE RESOURCES FOR INFORMATION SECURITY WITHIN YOUR ORGANISATION?



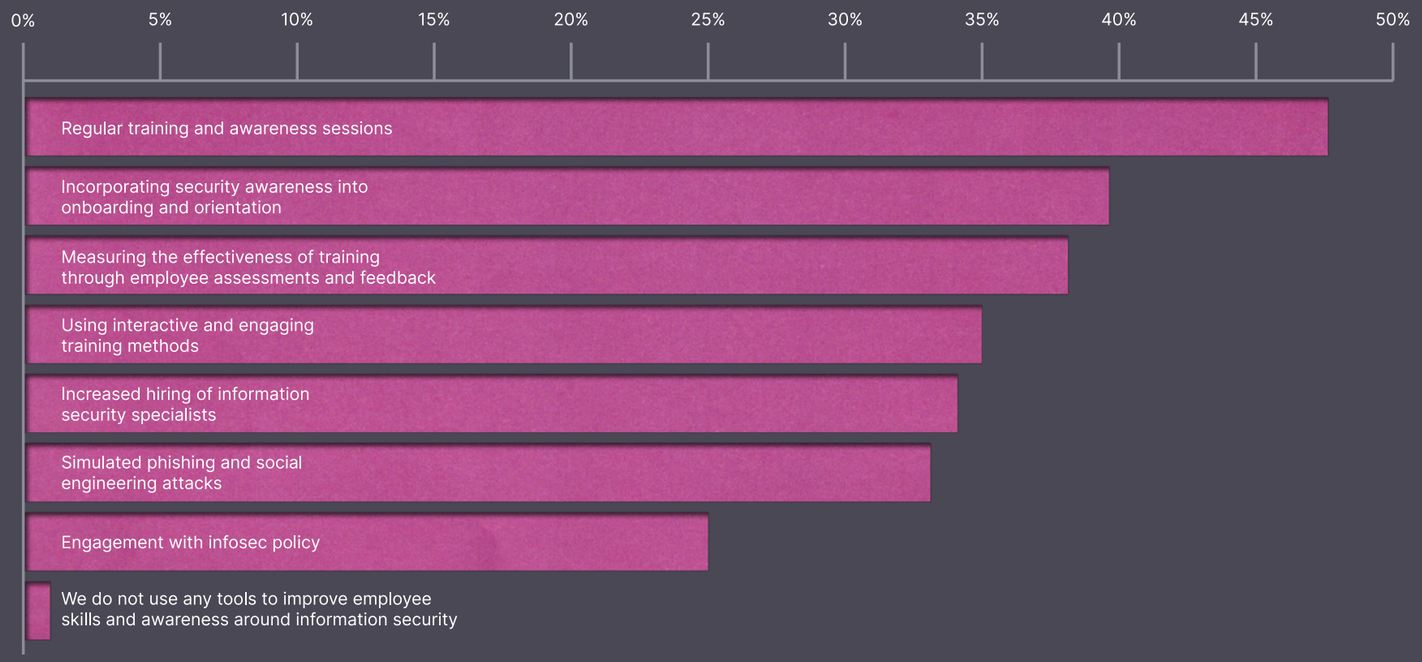
HOW DO YOU MEASURE THE EFFECTIVENESS OF YOUR INFORMATION SECURITY PROGRAM?

EMPOWERING PEOPLE TO STAY CYBER SECURE

While respondents listed regular training and awareness sessions as a top priority, the unusually high incidence of fines indicates that their response might have been something of a tick-box exercise. Surprisingly, respondents ranked engagement with their infosec policies (26%) as the least used tool to improve employee skills and awareness.

This low engagement level indicates that some leaders still view infosec as a cost rather than an opportunity. The survey showed that just 32% of respondents thought that senior leaders in their business viewed strong information security as a top priority.

WHAT TOOLS DO YOU USE TO IMPROVE EMPLOYEE SKILLS AND AWARENESS AROUND INFORMATION SECURITY?



According to the survey results, the three most common cyber mistakes employees make are:

CLICKING ON SUSPICIOUS LINKS OR ATTACHMENTS

28%

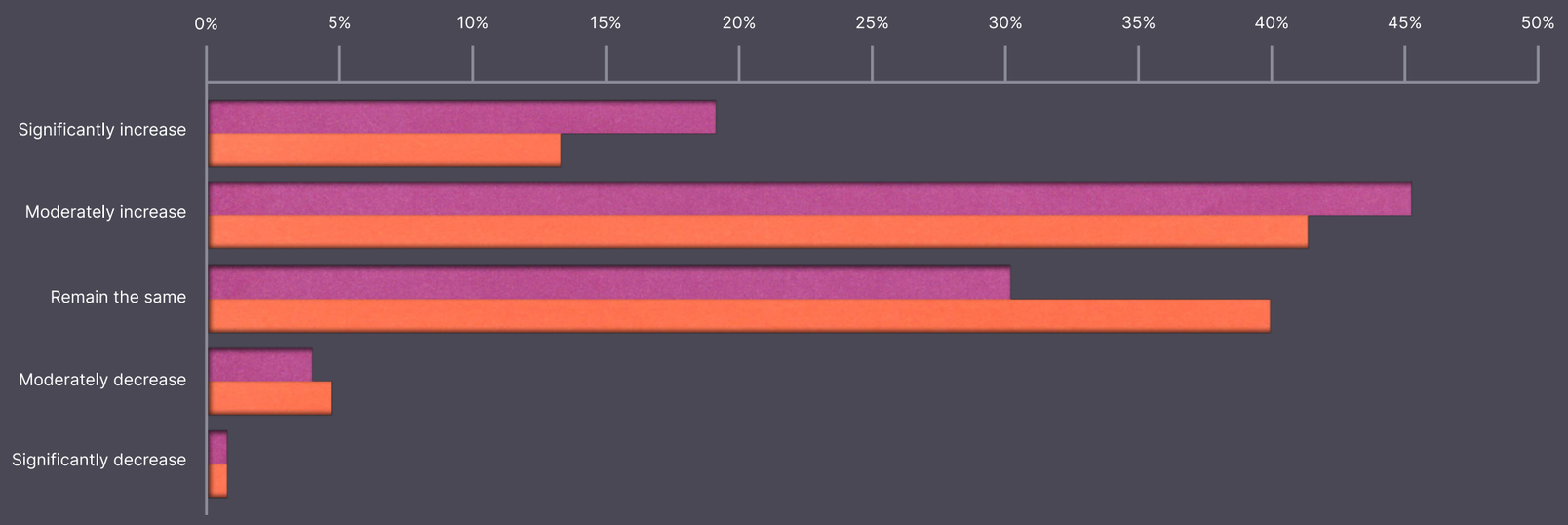
USING PUBLIC WI-FI NETWORKS FOR WORK PURPOSES

26%

USING WEAK OR EASILY GUESSABLE PASSWORDS

25%

HOW DO YOU EXPECT YOUR COMPANY'S OVERALL INFORMATION SECURITY BUDGET AND TEAM SIZE TO CHANGE IN THE NEXT 12 MONTHS?

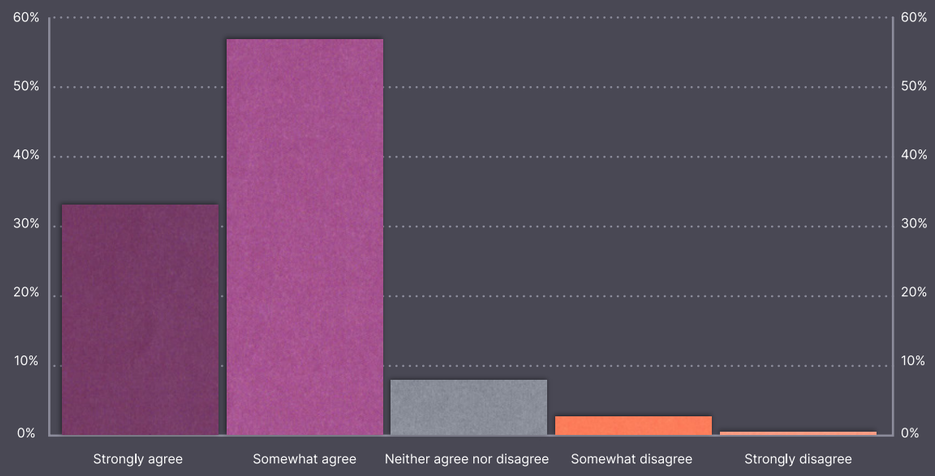


Just 32% of respondents thought that senior leaders in their business viewed strong information security as a top priority.

Therefore, organisations should provide regular security awareness training to ensure employees understand the importance of security and the measures they can take to protect sensitive information.

Given the increasing risk landscape and employee mistakes, it's surprising that many companies suggest they will not increase their budget or team size to help deal with infosec threats. In fact, 35% of companies said that their overall infosec budgets would stay the same, and 45% stated that their infosec teams would not grow over the next 12 months.

TO WHAT EXTENT DO YOU AGREE OR DISAGREE THAT OTHER SENIOR LEADERS IN YOUR BUSINESS VIEW STRONG INFORMATION SECURITY AS A PRIORITY?



UNDERSTANDING THE COMPLIANCE LANDSCAPE

Good security compliance helps protect a company's reputation and reassures its customers, ultimately driving business success. On the face of it, this seems straightforward. However, our research reveals two fundamental contradictions that need highlighting.

The first is that although only 27% of companies surveyed said they are struggling with regulatory compliance, our results show that, on average, it takes a company 15.5 months to obtain compliance with a single regulation such as ISO 27001.

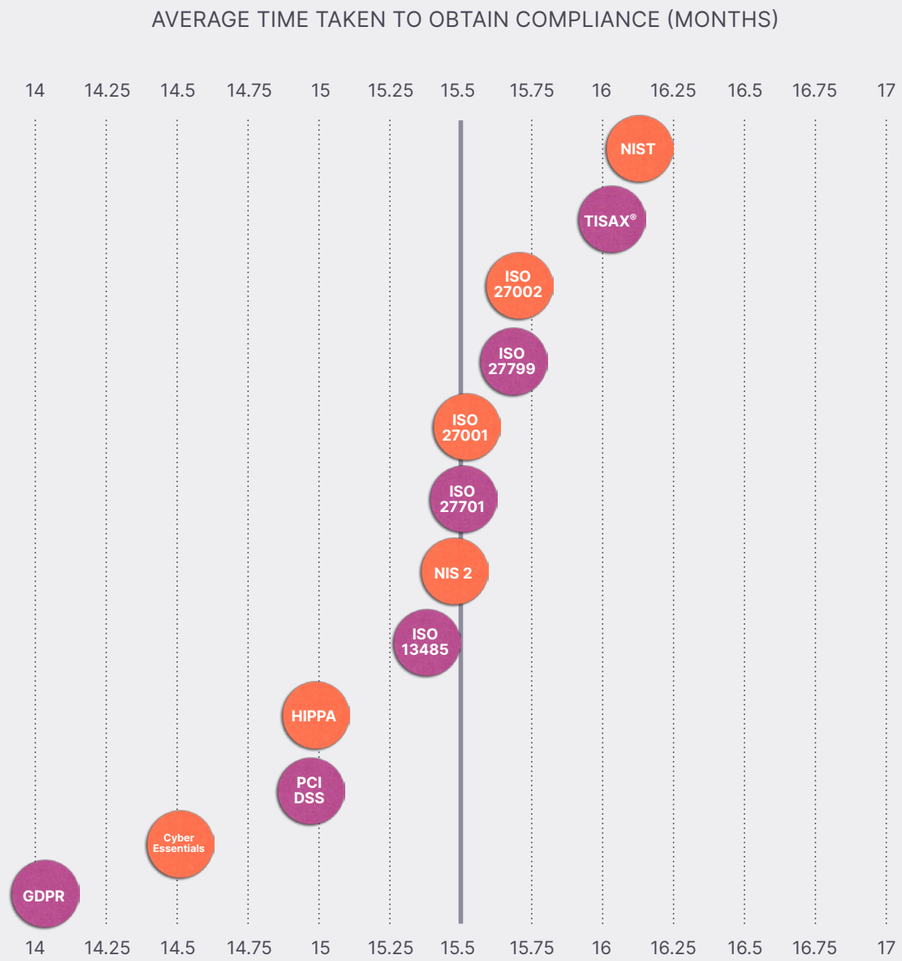
With the increasing pressure for companies to comply with both local and international regulations, this is clearly too long a timeline for companies to work with. This highlights the importance of leveraging software and people to accelerate compliance.

The second is the ongoing and constant threat of supply chain vulnerability. As organisations rely upon growing numbers of suppliers to deliver products, systems, and services, the risk of vulnerabilities being introduced or exploited via these suppliers increases significantly. Despite this, only 30% of respondents surveyed said they struggled with managing supply chain risk.

57% of companies surveyed have suffered at least one information security incident due to their supply chain in the last 12 months alone.

With that in mind, it's surprising that 57% of companies surveyed have suffered at least one information security incident due to their supply chain in the last 12 months alone. And in fact, many businesses have experienced more than one. This demonstrates the critical importance of robust information security in supplier relationships. Ultimately, a cyberattack like this can devastate a business, with expensive and long-term ramifications for affected organisations, their critical suppliers and their customers.

The survey results show that, on average, it takes a company 15.5 months to obtain compliance with a regulation such as ISO 27001.



Despite a greater focus on employee education and awareness viewed as one of the three top infosec opportunities, many companies still had a breach in the last 12 months showing there is still a long way to go.

CLEARING A PATH TO SCALABLE INFORMATION SECURITY

Hybrid working models, sprawling IT networks and the increased use of IoT solutions all necessitate new security approaches. The challenge lies in balancing the need for business innovation with the need for security.

Unsurprisingly, over half (55%) of respondents listed adopting new technologies such as AI, machine learning, and blockchain as top priorities and opportunities. However, the current hype surrounding these technologies could have skewed the response since investing in them alone is not a silver bullet. Competitive advantage also requires skilled talent, constructive data, and best practices.

The second opportunity listed is the growth of digital trust mechanisms. It aims to protect a business's data from fraud and bad actors to preserve client relationships, reputation, and revenue. Research conducted by McKinsey & Company in 2022 suggests that companies that succeed in building digital trust are more likely to boost their annual growth rates.

With human error still playing a significant part in many security breaches, the third highest opportunity for infosec leaders is a greater focus on employee education and awareness. This clearly demonstrates that not all the key opportunities centre around tech-based solutions.

Interestingly, most respondents (69%) don't see zero-trust models as an opportunity, presumably because they're commonly associated with challenges and not universally lauded as effective.

The next generation of CISOs entering the sector will view zero trust as a high priority.

But despite adopting a zero-trust security model being cited as the lowest priority (31%), the age-group results yielded a curious finding. A larger cohort of respondents representing the under-34 age group view adopting a zero-trust security model as a significant opportunity compared to their older colleagues. This is broadly consistent across the target industries and a possible indication that the next generation of CISOs entering the sector will view zero trust as a high priority.

Businesses will allocate equal money and resources to cloud security and employee security training and awareness. Nearly half of the respondents (48%) will conduct regular training and awareness sessions, while 40% will incorporate security awareness into onboarding and orientation sessions. Measuring training effectiveness through employee assessments and feedback will also be part of the mix. Yet, despite a greater focus on employee education and awareness viewed as one of the three top infosec opportunities, many companies still had a breach in the last 12 months showing there is still a long way to go.

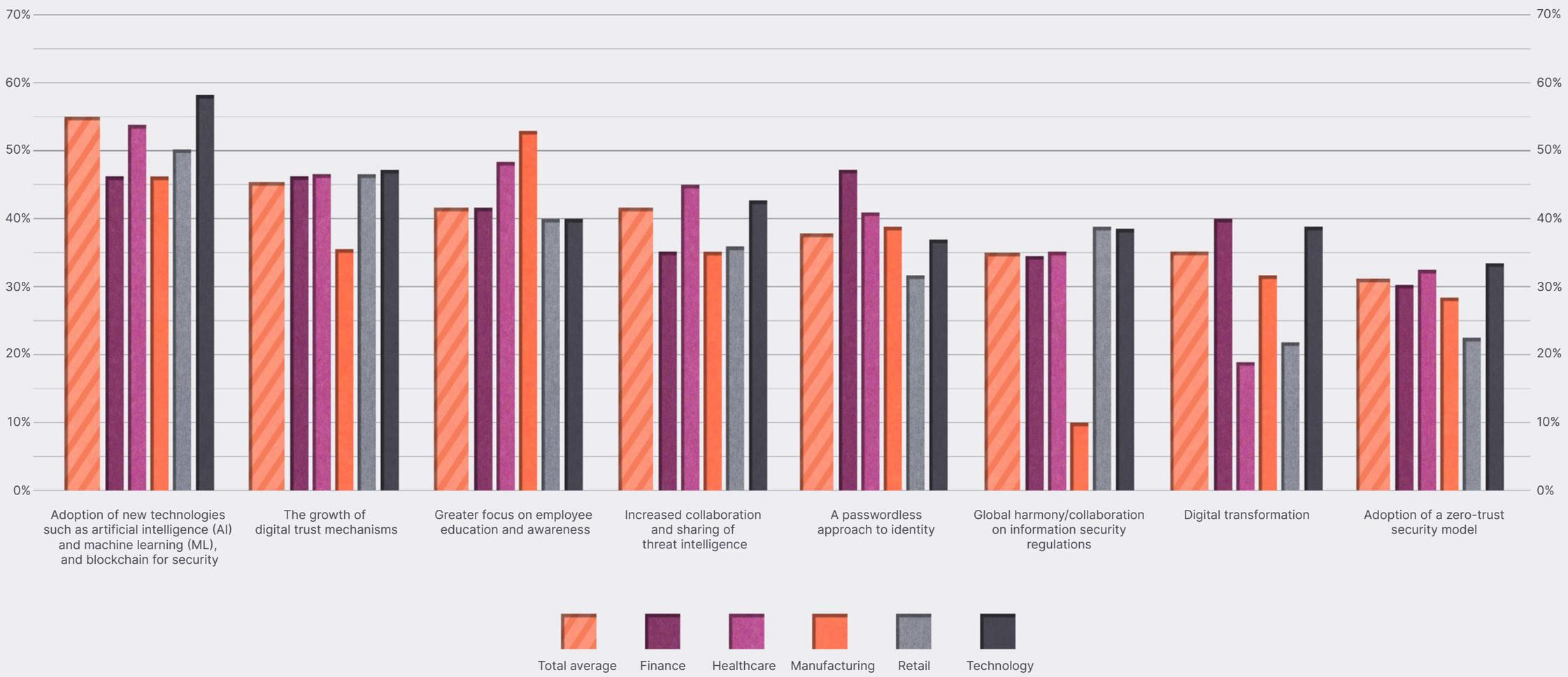
55%
Adoption of new technologies such as artificial intelligence and machine learning, and blockchain for security

45%
Growth of digital trust mechanisms

41%
Increased collaboration and sharing of threat intelligence

42%
Greater focus on employee education and awareness

WHAT DO YOU SEE AS THE OPPORTUNITIES IN INFORMATION SECURITY AT THE MOMENT?



LUKE DASH
CEO, ISMS.ONLINE

GOOD INFOSEC IS GOOD BUSINESS

In today's interconnected world, effective information and cyber security are no longer a "nice-to-have"; they're essential to business resilience and success.

Companies face increasingly sophisticated and frequent information security challenges, including cyberattacks, data breaches, and intellectual property theft. These risks can result in reputational damage, financial loss, and legal liability, making it more critical than ever for businesses to constantly adapt and improve their security measures to stay ahead.

From phishing attacks to malware infections and supply chain compromises, the volume and diversity of attack methods add complexity for organisations. It's no secret that attacks come in multiples, with most organisations facing more than three attacks per year on average. At the same time, organisations' infrastructures are increasingly spread across more platforms and services, requiring a greater volume of endpoints to be secured.

The consequences of these attacks can be severe, with fines for failure to protect data averaging over £250,000 in the last 12 months, not to mention the less easily calculable costs from reputational damage and customer compensation.

Simultaneously, cybersecurity regulations and compliance requirements are becoming more stringent, placing additional pressure on businesses to protect their data and systems. This can be particularly challenging for global organisations, with every country, state, and industry sector having slightly different requirements and specific intricacies within their regulations.

For any strategy to be effective, it must come from the top; senior leadership must drive a complete cybersecurity culture. Without that buy-in at the highest business level, any attempt to manage security effectively will likely fail.

But at ISMS.online, we believe these challenges can be overcome with a coordinated strategy that aligns your people, processes, and technology. We recognise the power of a comprehensive information and cyber security approach in tackling the cyber risk landscape. However, for any strategy to be effective, it must come from the top; senior leadership must drive a complete cybersecurity culture. Without that buy-in at the highest business level, any attempt to manage security effectively will likely fail.

We understand many organisations face tightening budgets and are expected to do more with less. Yet, investing in infosec does more than just protect information assets from costly breaches. It builds trust, wins business, and highlights efficiencies that make a real and measurable difference to the bottom line of every organisation.

SAM PETERS
CHIEF PRODUCT OFFICER, ISMS.ONLINE

UNLOCKING THE INFOSEC COMPLIANCE ADVANTAGE

Success is increasingly linked to information security in today's fast-paced business landscape. To futureproof your organisation and ensure sustainable growth, it's essential to demonstrate exceptional information security, data privacy, and cybersecurity standards.

Navigating this complex landscape can be challenging, but there are a few key things to remember. Firstly, your people are your first line of defence, so it's crucial to ensure they have the knowledge and tools to help protect your organisation. Secondly, effective processes and cybersecurity strategies are essential to mitigating risks, and finally, embedding technology which empowers your organisation to be more effective in cybersecurity is vital.

At ISMS.online, we believe that one of the most effective ways to achieve these goals is with an Information Security Management System (ISMS). An ISMS is a proactive approach to managing data. It helps you identify, assess, and prioritise your information security risks, implement mitigating controls, and ensure ongoing monitoring and review to stay ahead of changing risks.

Getting started can be daunting, so we built an all-in-one platform that enables organisations to achieve simple, sustainable security that can scale as you grow. Our ISMS is built on ISO 27001, a globally recognised framework that ensures you implement effective people management and embed effective processes alongside the technical controls for an ISMS.

As the cyber risk landscape evolves, organisations demonstrating their robust information and cybersecurity credentials will set themselves apart and unlock their growth potential.

ISMS.online is user-friendly and comes pre-configured to help businesses get over 80% of the way to compliance with ISO 27001. Our compliance platform also accommodates over 50 other regulations, industry standards and laws, including GDPR, ISO 27701, NIST, and HIPAA.

As the cyber risk landscape evolves, organisations demonstrating their robust information and cybersecurity credentials will set themselves apart and unlock their growth potential. At ISMS.online, we empower organisations to achieve simple, sustainable security that scales with your business as it grows, keeping you ahead of the ever-evolving cybersecurity threat landscape.

CONCLUSION

Smart business leaders are unlocking the potential of good infosec practices by placing information security at their organisation's core, realising business benefits and success above those without.

The report clearly highlights that organisations investing in their infosec culture, budgets and teams are materially less impacted by breaches or cyberattacks and the associated financial and reputational damage.

Placing information security at the core of a business establishes a foundation of digital trust. It empowers staff, customers and stakeholders to mitigate the risks companies face more effectively and maximises the opportunities it can offer through increased confidence, operational resilience and competitive advantage.

Protecting an organisation's digital reputation requires effective information security practices driven by senior leadership to establish an influential security culture.

In comparison, those organisations failing to invest in information security now experience more significant volumes of attacks and suffer more considerable financial and reputational damages. And the bad news, the cyber risk landscape is only becoming more complex, and the volume of attacks is increasing as cybercriminals operate as businesses in today's digital-first landscape.

Becoming a smart business means investing in infosec capabilities now. It starts with the right technology to help mitigate cyber risks and demonstrate compliance with all relevant regulations to establish a solid digital trust and cyber defence baseline. It requires effective processes to ensure the actions and responses to cyber threats are appropriate and proportional. And it means empowering your people to understand their role in securing your organisation's data and critical business assets; they are your first line of defence and one of your most powerful.

Protecting an organisation's digital reputation requires effective information security practices driven by senior leadership to establish an influential security culture. Those organisations that invest now will futureproof business growth and success.

ABOUT ISMS.ONLINE

ISMS.online is a leading SaaS company empowering every business to achieve simple, secure and sustainable data privacy and information security through its people-friendly platform.

Headquartered in the UK, with employees worldwide, ISMS.online has more than 12,000 users globally and works with a wide range of organisations — including enterprise brands like New Day, FDM, and Amigo.

isms.online