State of Cyber 2023/24

Security's Lament:

The state of cyber security in the UK

iomart


iOmart

“Organisations that establish a robust cyber security framework aligning with their strategy are well positioned to shape the future”

iomart

Welcome from Lucy

The second iteration of a research report is often the most interesting – having set a benchmark the first time around, it's always very useful to be able to see how things have changed and developed.

We've worked again this year with Oxford Economics, an independent research expert, to gather the opinions of 500 senior cyber security leaders and find out about their experiences over the last 12 months.

Many of the key issues we unearthed last year remain. Cyber leaders report a near-constant battery of attacks from online threat actors, compounded by increasing costs and tightening budgets. They face the unenviable balancing act of keeping their organisations safe, often with fewer resources.

The noisy landscape of technology solutions, including the breakaway star of 2022/23 – generative AI – can make it difficult to know how to optimise cyber defences.

What's concerning is that our research found an increase in the number of attacks over the last 12 months. The news headlines are still too frequently occupied by another household name which has suffered a successful breach. And for every one of these high-profile attacks, there are many more we don't hear about.

Our intention with this research is to help cyber decision-makers better understand the bigger picture of the threat environment and how others are approaching this pernicious challenge.

By working together and learning from each other, we can reduce our risk of falling victim to determined criminals – and more confidently take advantage of the growing benefits of a connected world.

We hope this report helps make those tough decisions a little easier.

Best wishes,

Lucy Dimes,
CEO
iomart Group plc

Contents

Introduction

Organisations that establish a robust cyber security framework aligning with their business and IT strategies are well positioned to shape the future. This alignment not only improves their resilience against today's inevitable, and often costly, cyber threats, but also fosters an environment favourable to innovation and revenue generation. Cyber security strategy has become integral to both the day-to-day functioning of business operations and the determination of potential growth.

Yet organisations are operating in an unpredictable landscape, with their efforts muddled by inflation, geopolitical tension, a cost-of-living crisis, and even advances in technology, such as generative AI. Bad actors are taking advantage of these circumstances—the past year saw a sharp rise in the average number of attacks over the year before. To make matters worse, despite upticks in the frequency and intensity of cyber attacks, many organisations cyber security strategies are still in their infancy, remaining at the periphery of their business processes. For companies to remain competitive or outperform their rivals, those strategies will have to mature rapidly. And they must overcome a cyber security talent pool that is running dry, as well as budgetary constraints, as cyber security competes for allocation against an abundance of other challenges.

The cyber security industry is also undergoing significant changes—as many new players enter the market and mergers and acquisitions consolidate suppliers. Despite the industry's complexity, though, organisations are eager to engage with it to get on top of their cyber woes, acknowledging the potential profit, reputation, cost, and efficiency benefits. To that end, many organisations have at least taken initial steps:

- Invested in cyber security services and products to understand points of vulnerability and manage threats;
- Introduced cyber hygiene and multi-factor authentication to create a culture of security; and
- Focused on employees, procuring training, and upskilling.

To take the pulse of cyber security, Oxford Economics and iomart surveyed 500 executives responsible for their organisation's cyber strategy. The sample includes executives from a range of industries—most with more than 1,000 employees—all based in the UK.

The survey revealed these key takeaways:

- Budgetary constraints hamstring cyber strategies in the face of increased incidents. A majority have an inadequate budget to fully protect their organisations at a time when many cite the increased cost of remediation as a major challenge. Rising insurance premiums can add to already strained budgets.

- There is a promising future for cloud and automation within cyber strategies. Businesses are increasingly investing in such technologies to bolster cyber security. With many concerned by shortages in their internal cyber skills and awareness, these technologies are seen as particularly pertinent given their importance to email screening and automated resolutions.

- While deploying the appropriate technology is crucial, effectively leveraging it requires the right people. The security skills gap yawns large and remains the biggest challenge for most cyber strategies. With internal skills and resources lacking, organisations face a major hurdle. To combat these obstacles and get the most from their tech investments, executives plan to invest in employee training while also hiring in-house specialists and third-party consultants.

Methodology/demographics and key definitions

- **Sample:** Cyber security strategy decision-makers (n=500)
- **Executive titles:** CTO, CIO, CISO, CFO, COO, Chief Digital Officer, CEO, Chief Risk Officer, Chief Data Officer
- **Sectors covered:** Software, Professional services, Legal, Finance, Not-for-Profit, Government, Insurance, Healthcare, Manufacturing, Retail, Transportation, Consumer products
- **Company sizes represented:** Most respondents have more than 1,000 employees. 20% have £250 m to £499 m in revenue, 20% have £500 m to £999m in revenue, 20% have £1bn to £4.99bn in revenue, 20% have £5bn to £9.99 bn in revenue, 20% have more than £10bn in revenue.
- **Locations covered:** Respondents are all from the UK
- **Dates fielded:** July 2023

Part 1: Balancing threats and budgets

Phishing
56%

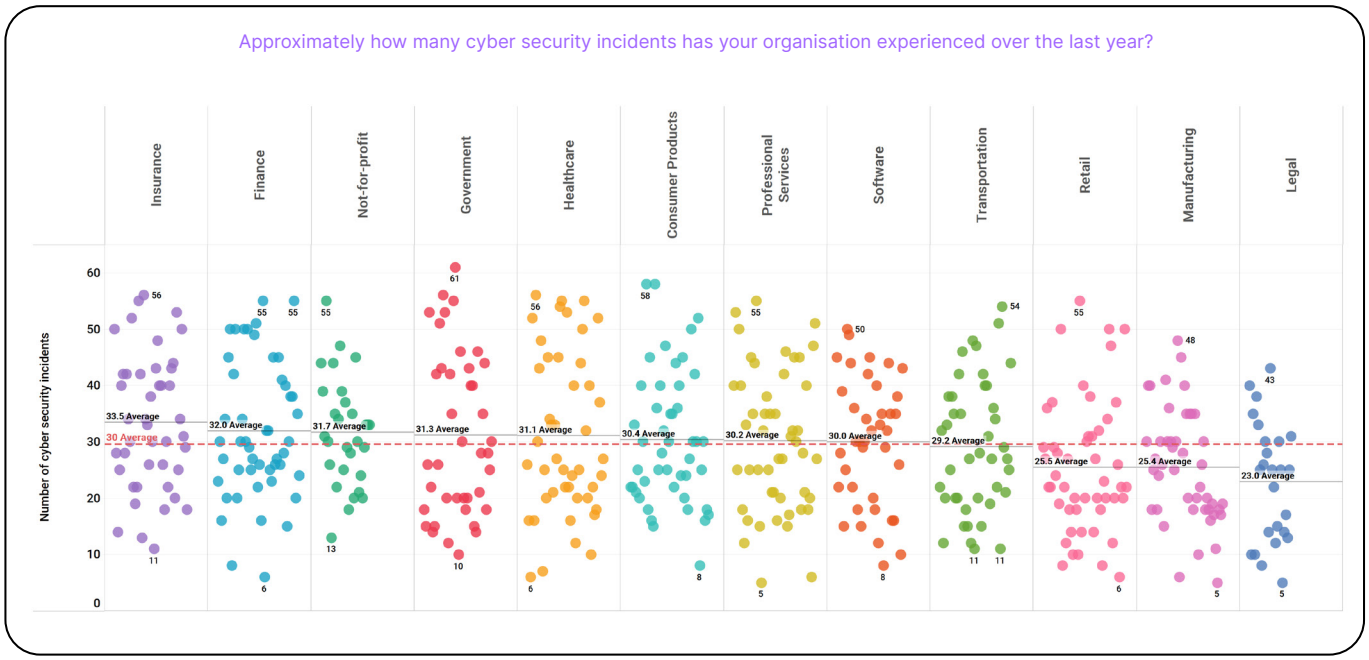
Malware
55%

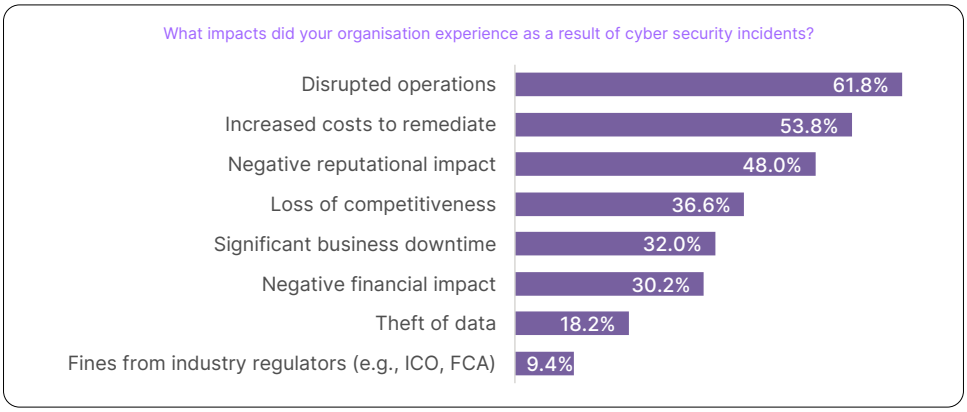
remain the threats of greatest concern to executives for the second year in a row

Threats are constantly evolving. More than a third of decision-makers say keeping up with the pace of evolving threats is a top challenge. Over the last year, organisations experienced an average of 30 cyber incidents, which represents an annual increase of six incidents over the 24 reported last year. And these are the ones organisations know about.

Not surprisingly, phishing (56%) and malware (55%) remain the threats of greatest concern to executives for the second year in a row, and less than half are confident in their organisation's ability in handling them (49% phishing, 48% malware). Fewer still (one quarter) are sure of their ability to deal with ransomware—a threat that continues to dominate headlines globally. Not to mention disruptions from the past three years continue to complicate their ability to protect themselves—executives are struggling with managing increased volumes of data, the pace of technology, and supply chain disruptions within their security strategy.

Keeping pace with threats is more important than ever. To respond, or even become more proactive, organisations are looking to improve





their cyber postures, allocating an average of £40,190 to vulnerability assessments, penetration testing, or red team engagements. However, they are also fully aware these measures alone are not sufficient, and they need more money to underpin their plans. More than a quarter (27%) of organisations think their current cyber security budget is inadequate to fully protect them from emerging threats.

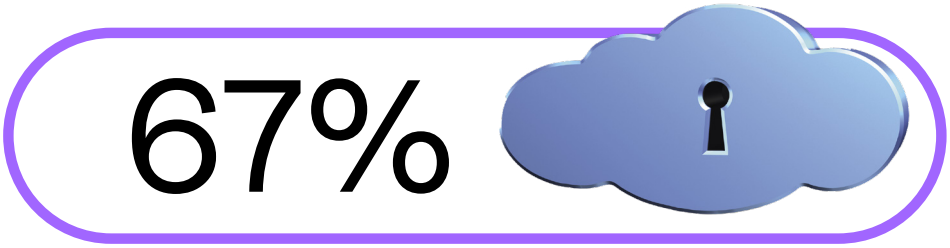
But budgets hamstring efforts. Tight budgets continue to be a top barrier in meeting cyber security goals, and rising cyber insurance premiums only stress budgets further. The increase in cyber premiums is ranked as the top change over the past two years, with 70% of respondents noting a rise and just 4% seeing a decrease. The uptick in pricing only adds to the cost of remediation, with the majority (54%) of respondents suggesting it is the second greatest impact of cyber security incidents, well above more traditional factors such as theft of data (18%) and negative financial impact (30%).

And the tightening of budgets creates blind spots. With 41% of organisations being forced to sacrifice cyber security to keep the lights on during the pandemic, it is no wonder cyber security initiatives are not evenly applied across businesses. Only 37% of respondents agree that security is embedded into all their business processes and functions, while 14% admit that security is addressed on an ad-hoc or as-needed basis.

70%

say rising cyber premiums is the top ranked change over the past two years

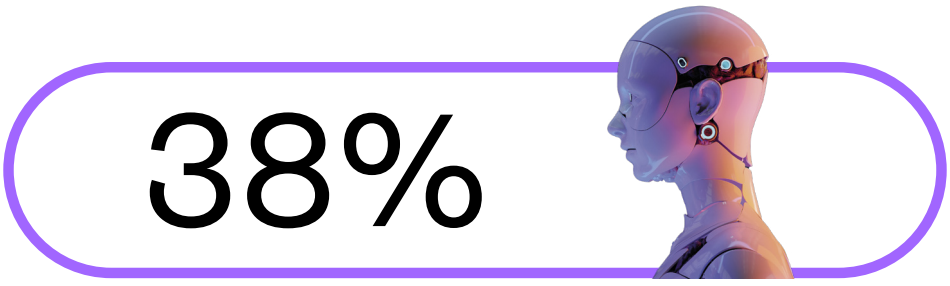
Part 2: Tech has become increasingly integral to a strong cyber strategy



say private cloud has strengthened their security

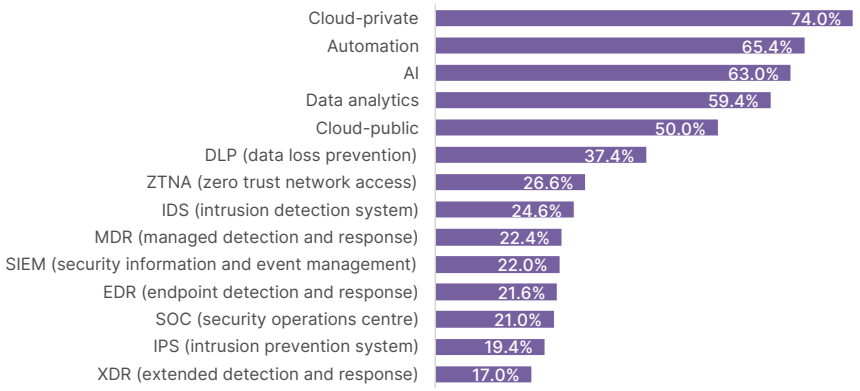
Leveraging existing technology. Executives may be feeling the crunch, but creating a strong cyber strategy on a tight budget is not impossible because some of the groundwork has been laid. Many organisations already have the technology to help them keep up. Cloud has become foundational to cyber strategies—almost three-quarters (74%) of organisations rely on private cloud, with 67% saying it has strengthened security. And nearly two-thirds (65%) lean hard on automation. More than half (53%) will use automated responses over the next two years, while 51% plan to employ both SIEM monitoring and automated resolution of security incidents.

Emerging tech comes into play. Despite a focus on well-established technologies, many executives also place considerable faith in emerging technologies. Well over one-third (38%) believe the increased use of AI and ML in threat detection and response will be a significant trend in cyber security over the next two years. In particular, they cite email screening (78%) and contextual analytics (69%) as dominant use cases for AI and automation. However, budgetary concerns (31%), compliance and regulatory requirements (23%), and a lack of skilled workers (23%) are obstacles to successfully implementing nascent technologies such as AI and automation.

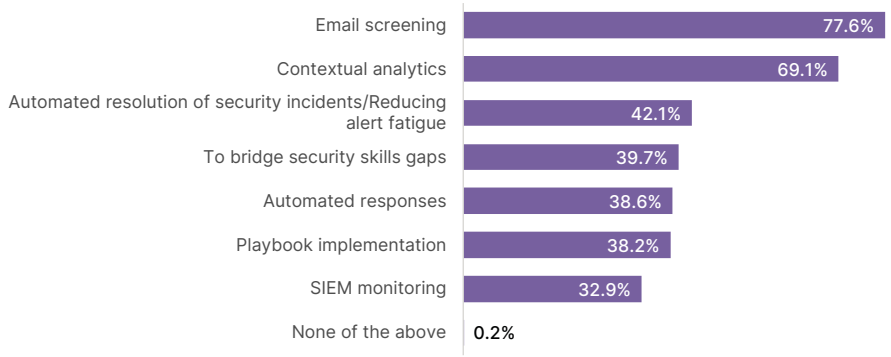


believe the increased use of AI and ML in threat detection and response will be a significant trend in cyber security

Has your organisation implemented, or does it plan to implement any of the following technologies to increase cyber security?



For which of the following cyber security tasks do you currently use AI or automation?



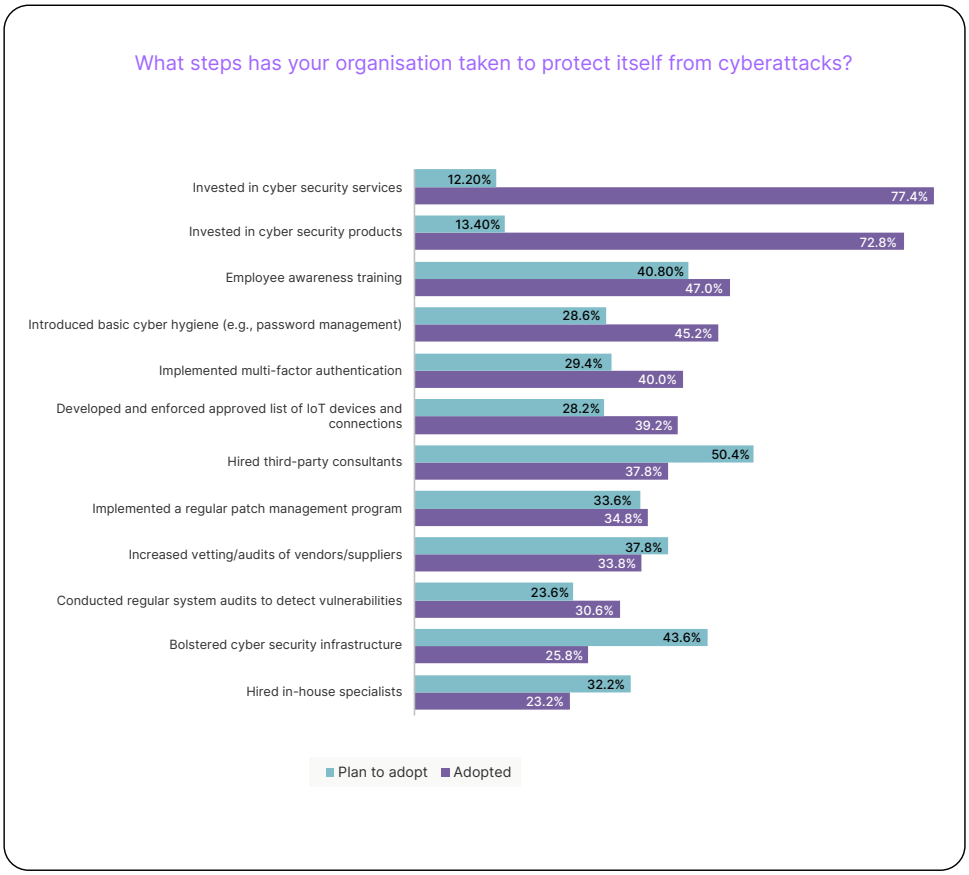
Managing the tech shift. Figuring out where to start investing has proven difficult. Our survey found that executives have trouble sorting through the "noise" created by the tsunami of offerings and security players in the market to find the best fit for their organisations needs and budgets—nearly two in five (38%) struggle with this. While most are generally enthusiastic about tech adoption—almost all respondents have invested in new products — only half say their investments have been effective. Purchasing tech and cyber security products without a clear strategy and people who can leverage it effectively diminishes its potential. To maximise the value of their investments, executives need guidance on navigating the shift to an increasing reliance on technology.

Part 3: Talent is crucial in combatting threats

53%

say cyber security culture and regular employee training to prevent human-related breaches will be crucial

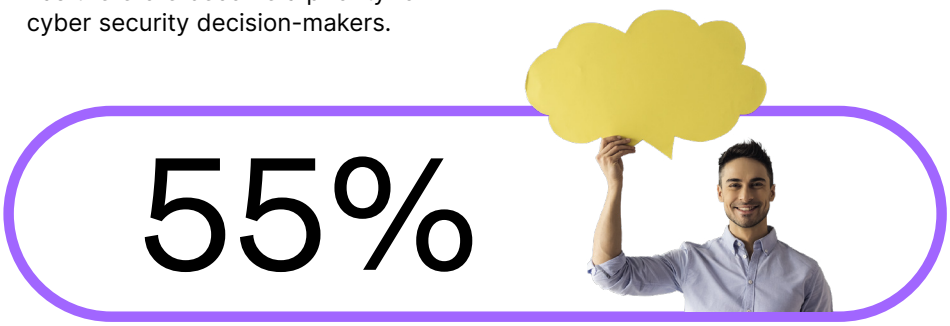
People are key to cyber success. As important as tech is to cyber security, executives are looking to their employees to be the first line of their cyber defence. More than half (53%) say cyber security culture and regular employee training to prevent human-related breaches will be crucial, indicating the continuation of a significant trend. In the past two years, 63% of organisations have invested in employee training.



But getting people in place takes effort. Putting the right people in place is complicated by skills gaps and a continuing shortage of skilled workers. Decision-makers say a lack of internal skills and resources constitutes the biggest challenge in meeting their cyber security goals. With burnout among cyber security staff on the rise—30% believe their teams are suffering from it—getting the right talent (and the right technology to support them) is more important—but harder—than ever.

Flexible and hybrid work, a well-established work lifestyle for many office employees, has also introduced new challenges and vulnerabilities. Almost half of respondents (46%) say the bump in remote and flexible work—and a more geographically distributed workforce (36%)—have complicated their organisation's ability to protect against cyber threats. It is no wonder then that few feel confident in tackling their greatest cyber security threats and that reducing cyber risks created by employees has therefore become a priority for cyber security decision-makers.

Getting the right people. To close some gaps—outside of upskilling and reskilling employees—almost a third of organisations (32%) will hire in-house cyber security specialists in the next two years, and a full half (50%) will do the same for third-party consultants. Executives also are eyeing non-traditional talent sources to overcome skills shortages—75% plan to hire from less-traditional pools of job candidates, such as gamers and ex-military. And more than half (55%) plan to expand cyber fluency to the top of the corporate ladder by stocking boards with people who have specific cyber security experience . Even more (72%) will create internships and apprenticeships. These steps are important to creating a more cyber security literate workforce that can successfully implement cyber strategy and leverage the technology investments associated with it.



plan to expand cyber fluency to the top of the corporate ladder by stocking boards with people who have specific cyber security experience

Meet the cyber security strategy leaders

We isolated a group of survey respondents who are using technology and talent to get the most from their cyber security investments. This elite group (n=126, approximately 25% of the sample) is defined by the following:

- Respondents in the first quartile who have already implemented initiatives like employee awareness training, introducing basic cyber hygiene, hiring third-party consultants, using managed service providers, using technologies like AI and automation, and aligning their strategy with business and IT.
- They have implemented a stronger talent strategy, like improving employee skills, using managed service providers and professional services, and bringing on board members with specific cyber security experience. They are far less likely to say their internal cyber security teams are suffering from burnout.
- They experience better results from their efforts. They are more likely than others to say initiatives like employee awareness training, introducing basic cyber hygiene, investing in the right products and services, and bolstering cyber security infrastructure have been effective.
- They manage data better than other respondents—almost all are confident in keeping up with data regulations, preventing data security breaches, and sharing data internally with partners.
- They have made purposeful investments in technology—most have invested in cloud and updated infrastructure, as well as AI and automation, potentially to close some skills gaps.
- They are less likely to say their budget is inadequate to fully protect their organisation.
- They're already reaping the benefits of their efforts—they've already seen improved profitability and cost savings, internal efficiency, and revenue, and increased innovation potential.

The takeaway: balancing tech and talent like our Leaders could give organisations a leg up when setting cyber strategy.

Part 4: How does my industry stack up?

Finance and Insurance are still working out the kinks. There are stark differences between industries when comparing the number of cyber incidents they experience annually. On the high end of the spectrum sits Insurance, Finance, Not-for-profit, Healthcare, and Government, all seeing at least 31 incidents a year. Insurance, with the second highest number of incidents last year, reported the highest number of incidents this year, despite spending the second highest amount on cyber testing and assessments (£46,100 on average vs. £40,190 total). Finance fell from first place last year in the number of incidents they experience but is still comparable to Insurance. Organisations in this space face similar challenges, such as budget limitations, and agree there are too many cyber security products and services on market. Consequently, like those in many other industries, the Finance sector emphasises the increasing importance of cyber security culture and regular employee training to prevent human-related breaches.

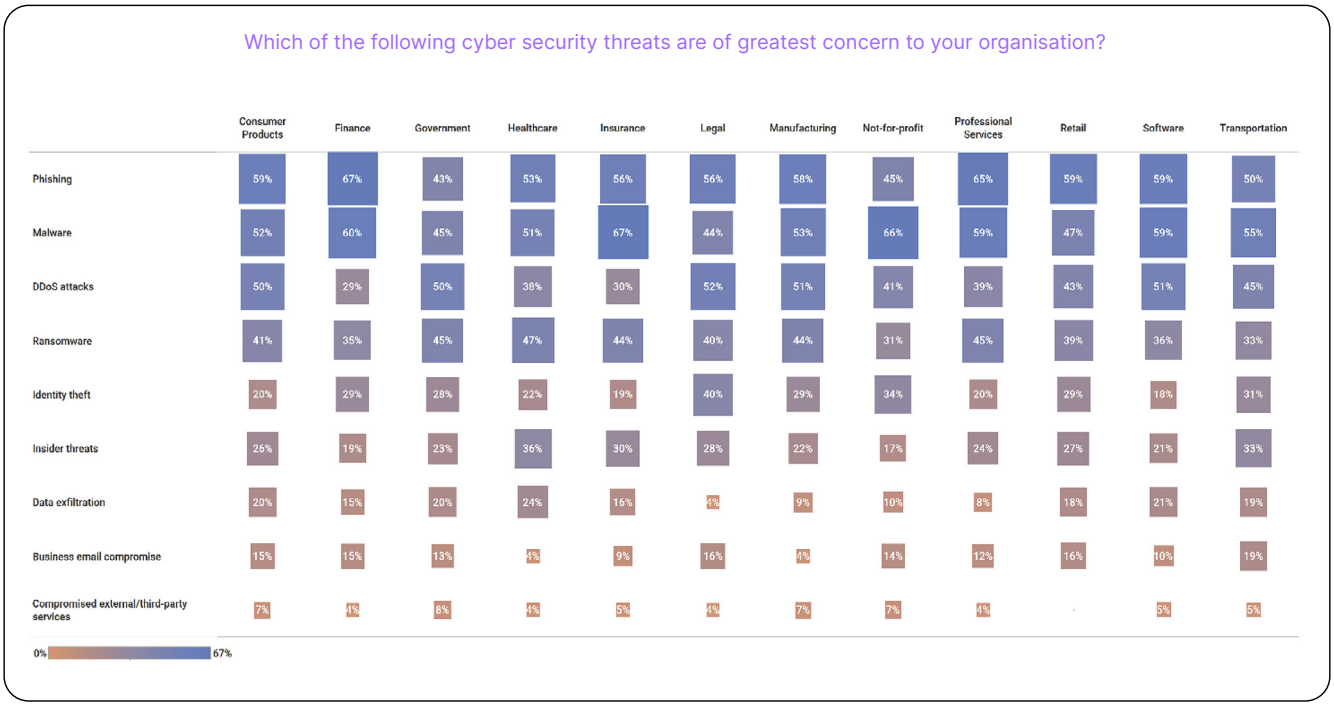
The Public Sector is struggling to keep up. UK Public Sector organisations in Healthcare and Government are in a similar boat. Both are more likely to say cyber security threats have increased in frequency over the last two years (56% of Healthcare, 55% of Government vs. 48% of the survey total). In recent months, the UK Public Sector has been battling a wave of ransomware attacks, with critical infrastructure like the NHS Trusts, Ofcom, and pension services, all being targeted. Ransomware reasonably is by far their top concern, much higher than any other industry.

The Public Sector is also feeling the effects of cyber skills shortages at higher rates than the Private Sector, a potential explanation of why it is struggling to mitigate threats. Executives in this space are more likely to say it is harder and more expensive to find and retain cyber staff (38% of Healthcare, 48% of Government, vs. 34% survey total). Going forward, however, the Public Sector plans to invest in employee awareness training over hiring third-parties, in-house specialists, or purchasing insurance.

Manufacturing forges ahead. On the other end of the spectrum is Manufacturing, which, for the second year, has reported one of the lowest rates of cyber security incidents, at an average of 25 per year. Despite digitalisation deeply transforming the industry—and opening it up to cyber threats—executives in this arena are slightly less likely to say incidents have increased in frequency over the last two years (44% vs. 48% total). The reasons behind the industry's seeming success range from the high-level strategic decisions to lower-level tactical and operational ones. Strategically, Manufacturing executives, compared to those in other industries, are significantly more likely to have embedded security into critical infrastructure and aligned cyber security and IT strategies. Tactically, they have gone to greater lengths to mitigate cyber risk by investing in cyber security products, outsourcing intelligence, introducing basic cyber hygiene, and purchasing comprehensive cyber insurance. Finally, operationally, they are more likely to conduct employee awareness training and implement multi-factor authentication.

These factors may all be underpinned by the benefits accrued from hiring from less traditional talent pools (29% vs 21% average). Despite current success, Manufacturing fully acknowledges the targets they have on their backs and are not complacent. The industry is also more likely to plan to hire third-party consultants, bolster cyber security infrastructure, implement a regular patch management program, and hire in-house specialists.

Annually, how much do you spend on vulnerability assessments, penetration testing or red team activities?



Conclusion

Talent and technology should go hand in hand to ensure an effective and agile cyber security strategy. But that is easier said than done—an advanced cyber strategy continues to evolve and grow in complexity, making it difficult to figure out where to start. Executives must implement the technologies with intention, ensuring their investments suit their organisation's specific needs and are used effectively. To create a robust cyber security strategy and reap the benefits of those efforts, we recommend organisations take the following actions:

- **Invest in the right technology solutions** . It seems so simple, but with an array of technological solutions on the market, it can be difficult to assess the best fit for your organisation—and often newer fixes aren't compatible with legacy infrastructure. Avoid panic buying and throwing precious budget down the drain by understanding where your gaps are—whether it's bolstering cyber security or improving employee skills— to decide where your tech investments should be targeted.
- **Ask for help.** Understanding those gaps is easier said than done—and investing in the right solutions is even scarier when budgets are tight. To maximise your budget, hiring a third-party advisor or in-house consultant can point you in the right direction. Seeking advice on this can help you avoid making inappropriate investments and can recommend what should be done with existing technology—and even employees.
- **Bring your employees with you.** While investing in the right technology is crucial to improving your cyber strategy, the need for human oversight is even more important. You need a team that has awareness of both the complexities and significance of a strong cyber strategy—and you need them to implement it successfully. Whether it's upskilling and reskilling employees or bringing in people with specialised skills, there are many ways your employees can become a key line of defence in combatting threats.


iomart

"While investing in the right technology is crucial to improving your cyber strategy, the need for human oversight is even more important".

iomart

Welcome to straightforward → iomart.com

iomart Group plc. 55 Robertson Street, Glasgow G2 8JD