# UNDERFUNDED AND UNDER-REPORTED:

# THREATS, BREACHES AND BUDGETS

WWW.RIVERSAFE.CO.UK

RIVERSAFE

# SUMMARY OF CONTENTS


- Introduction ..... pg3
- Threats and breaches..... pg4
- Funding defences ..... pg5
- Skills, tools and other challenges..... pg6
- Conclusions and actions ..... pg7


## METHODOLODY

RiverSafe commissioned independent polling agency Censuswide to survey 250 cyber security professionals at CISO (Chief Information Security Officer) level or equivalent across UK businesses. The research was equally weighted to all areas of the country and took place in January 2024.

# INTRODUCTION

Today's organisations are up against a multitude of challenges. Economic uncertainty, talent shortages, and geopolitical unrest are throwing up obstacles for businesses and institutions across every industry as they strive to deliver their services.

The last thing any organisation needs to deal with is a cyberattack—but with a cyberattack being launched every 39 seconds, it's highly probable that they will experience one.

Exacerbated by AI and a growing attack vector, cyber threats are getting more frequent, more sophisticated, and more damaging every day. These attacks are set to cost the world $9.5 trillion in 2024.

No matter how big or small, organisations cannot afford to put cybersecurity on the backburner. But in a fast-evolving threat landscape, how we go about defending ourselves against cybercrime matters more than ever.

Even with the best firefighting equipment at hand, it's always better to stop a fire from starting at all. So, to help organisations understand what they're up against and be better prepared to defend their digital assets, we asked CISOs from across the UK about their current cyber strategies, the biggest challenges they're facing, and what they're doing to fight back.

In this report, we'll outline some of the key findings from our research, explain the trends and reasons behind them, and share expert tips on how businesses can strengthen their security posture against a growing torrent of cyber threats.

We hope you find this report useful.

# THREATS AND BREACHES

The pandemic has rapidly accelerated the shift of businesses to online platforms, expanding the attack surface and increasing the chance of more complex and widespread attacks. Last year, 26 percent of organisations suffered a cyberattack.

17 percent of respondents admitted that their company failed to report a cybersecurity breach that occurred last year. A concerning number, but not just for legal, regulatory, and financial reasons, cyberattacks and data breaches should be reported. Especially when it comes to cyber-security, knowledge is power, and without a true and complete picture of the threat landscape, we're at even more of a disadvantage in our efforts to fight back.

75 percent of respondents believe that insider threats pose as a greater risk than external threats to their organisation. Insider threat incidents are on the rise, with occurrences spiking by 47% over the past five years with the average cost in 2023 of an incident being around $15.38 million.

Despite this, 64 percent claim their organisation doesn't have sufficient technology to protect against insider threats. Insider threat incidents are on the rise, with occurrences spiking by 47% over the past five years. There are a number of reasons contributing to this alarming growth.

One of which, 20 percent admit that an employee at their organisation exposed company data using AI tools such as ChatGPT, with a further 20 percent identifying AI as the biggest cyber threat, pointing to concerns over AI's potential use as part of cyberattacks.

"AI is already being used in malicious cyber activity and will almost certainly increase the volume and impact of cyber-attacks- including ransomware- in the near term." – National Cyber Security Centre (NCSC).

AI is being used to enhance or evolve existing attack methods, making them not only more effective but also modifying them to make it more difficult for antivirus software, spam filters, and other cybersecurity measures to detect them.

**ADMIT THAT AN EMPLOYEE AT THEIR ORGANISATION EXPOSED COMPANY DATA USING AI TOOLS SUCH AS CHATGPT**

# FUNDING DEFENCES

We asked our CISOs how they're budgeting for their cyber defences this year. Awareness around the need for greater investment is on the rise, though the majority of security leaders feel that they're still not being given enough resources to tackle the problem.

90 percent of organisations will be increasing their investment in cybersecurity this year. Investment in cybersecurity is going up almost across the board, with just 10% of respondents reporting that spending will remain at previous levels or even decrease.

Despite the significant breadth of investment mentioned, 59 percent of respondents feel their organisation still isn't investing sufficient resources into cybersecurity.

Given the growing number and sophistication of cyberattacks that CISOs are witnessing on a daily basis, it's no surprise that many feel they don't have enough budget to work with. During the 2022-23 budget cycle, cybersecurity spending growth dropped 65 percent.

With organisations struggling to stretch their cybersecurity budgets, could AI offer a solution? 87 percent of organisations are implementing automation to achieve cost savings.

Clearly, finding ways to work smarter rather than spending more is going to be a big challenge for cybersecurity leaders in the coming year. 43 percent of our respondents are investing more in automation processes this year- a step that, if done properly, can have a massive impact on productivity and performance.

According to IBM Security's 2023 Cost of a Data Breach Report, investing in automation helps deliver shorter breach lifecycles and a more resilient security posture—which is good news for short-staffed teams dealing with a skyrocketing number of attacks.

AI undoubtably offers many benefits for a cybersecurity team looking to prioritise their spending, but can it be a double-edged sword? 65 percent believe that AI has limited their cybersecurity budget.

This belief that AI can be a cure-all will seem far-fetched to cybersecurity professionals, but for executives looking for any way to cut costs, it may provide a reason to limit budgets. Reducing budgets and expecting AI to pick up the slack is a problematic strategy, not only because high-quality, secure AI solutions themselves cost money, but also because many cybersecurity teams are already on the backfoot when it comes to proper funding.

**OF ORGANISATIONS WILL BE INCREASING THEIR INVESTMENT IN CYBERSECURITY THIS YEAR**

**OF RESPONDENTS FEEL THEIR ORGANISATION STILL ISN'T INVESTING SUFFICIENT RESOURCES INTO CYBERSECURITY**

# SKILLS, TOOLS AND OTHER CHALLENGES

We asked our CISOs what kind of obstacles they felt stood in the way of building a robust cybersecurity posture in their organisations. Their answers underlined three major challenges: talent, tools, and time.

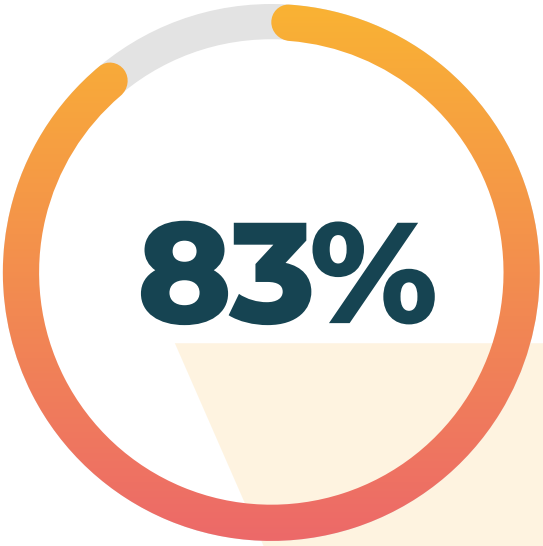
According to our respondents, the biggest challenge for cybersecurity leaders is finding the right talent for their teams. 83 percent of respondents feel their organisation has a gap in its cyber skills.

In the UK, the number of cyber security job postings increased by 30% in 2023. Despite the high salaries on offer, the cybersecurity industry has struggled to attract and train enough new professionals to meet rising demand. This lack of available talent is leading businesses to try alternative ways of accessing critical skills, such as outsourcing and internal upskilling.

It appears it's not just high salaries preventing organisations from building their own internal cybersecurity teams. 60 percent revealed that investing in hiring and training dedicated cyber-security staff is draining too many resources.

The difficulties organisations face around hiring, retaining, and training internal cybersecurity staff could indicate why just 32% of respondents said their organisation had its own in-house security operations centre (SOC) team.
An SOC is an essential factor in maintaining a robust cybersecurity architecture. A SOC can oversee real-time monitoring, identifying and prioritising threats, and ensuring fast and appropriate responses to any potential incidents detected by its tool stack.

Adequately protecting an organisation from cyberattacks requires having full visibility across every inch of the digital environment, but 63 percent of respondents admitted that their organisation doesn't have enough visibility over devices. This lack of clarity creates dangerous blind spots, making organisations more vulnerable to attack and less able to respond quickly in the event of a serious security incident.




**OF RESPONDENTS FEEL THEIR ORGANISATION HAS A GAP IN ITS CYBER SKILLS**

# CONCLUSIONS AND ACTIONS

Thanks to AI and an ever-expanding attack vector, cyberattacks are becoming more common, more sophisticated, and more difficult to defend against. Every organisation is a target, and businesses must adopt a when, not if, mindset when it comes to cyberattacks.

**Here are our top three recommendations based on the research:**

1. **Tackling new and growing threats** - AI is here to stay and businesses must revisit their cybersecurity strategies to ensure they're prepared for new, AI-powered threats. Whether it be dedicating more resources to tackle insider threats across all fronts, especially employee negligence or conducting up-to-date employee training that helps staff understand the dangers of new breeds of attack, such as advanced phishing, and recognise them when they see them

2. **Stretching the budget** - Even despite economic uncertainty, getting maximum value from cybersecurity investments will be a major driver in 2024—and many will look to automation to help them achieve this. Implementing robust data management, routing and storage practices to ensure the security and integrity of critical information will minimise the risk of breaches or unauthorised access.

3. **Implementing tools and talent** - To properly protect an organisation in an evolving threat landscape, accessing and fully exploiting the necessary resources is essential. To build a well-equipped and adequately resourced SOC, businesses can invest in automation to reduce time spent on manual processes, increase productivity, while freeing employees up to work on more complex tasks. By evaluating your tech stack, businesses can focus on integrated tools. That can streamline security operations and perform multiple functions.

# CYBER SECURITY SOLUTIONS

## BUILD A RESILIENT ENTERPRISE AND PROTECT BUSINESS CRITICAL ACTIVITY

Get in touch to arrange a cyber security consultation with our team.

**www.riversafe.co.uk**