AI UNLEASHED:
NAVIGATING CYBER RISKS

WWW.RIVERSAFE.CO.UK

RIVERSAFE

SUMMARY OF CONTENTS

METHODOLOGY

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 June 2023.

INTRODUCTION

The rapid rise of AI adoption is set to transform the way businesses operate beyond all recognition. From the deployment of advanced chatbots such as ChatGPT to produce content and research, to harnessing the power of AI to improve education and healthcare, the technology will impact every aspect of our daily lives.

Yet the debate continues to rage around whether AI is a force for good or a worrying development that will put jobs and livelihoods at risk. The World Economic Forum's **Future of Jobs report** published this year suggests that 50% of companies globally expect AI to create job growth and 25% expect it to create job losses between 2023 and 2027.

Whatever your opinion, the reality is that machines will continue in one form or another to manage greater and more complex workloads for the foreseeable future. Inevitably, this will include managing and distributing confidential data as well as personal information.

Against the backdrop of rising levels of cyber crime, including ransomware attacks that are increasing in terms of volume and sophistication, the security issues around widespread AI adoption require urgent attention.

In the last year alone, **government research** suggests that across all UK businesses, there were approximately 2.39 million instances of cyber crime and approximately 49,000 instances of fraud as a result of cyber crime in the last 12 months. With this in mind, the case for further investigation of the risks associated with AI adoption, data management and cyber security is clear.

To explore this issue in greater detail, RiverSafe has commissioned independent research company Censuswide to poll 250 cyber security industry leaders about their thoughts on the threat AI poses to their organisation. By asking the very people tasked with keeping their organisation safe from outside threats, we hope that this report will offer valuable insights, data and guidance for those looking to improve their cyber defences in an AI-enabled world.

We hope you find this report useful.

Suid Adeyanju
CEO, RiverSafe

PART 1: RISING RISKS

Once a major event, cyber breaches are now so commonplace that for many organisations the discussion is about when rather than if they will face an attack. From national infrastructure and international businesses to charities and garden centres, hackers show no mercy to their victims.

Indeed, **government figures show** that 32% of businesses and 24% of charities overall have experienced a breach or attack within the last 12 months. This is much higher for medium businesses (59%), large businesses (69%) and high-income charities with £500,000 or more in annual income (56%).

To understand the state of cyber readiness in UK business, we asked respondents to tell us in detail about the measures they had in place to prevent a cyber attack.

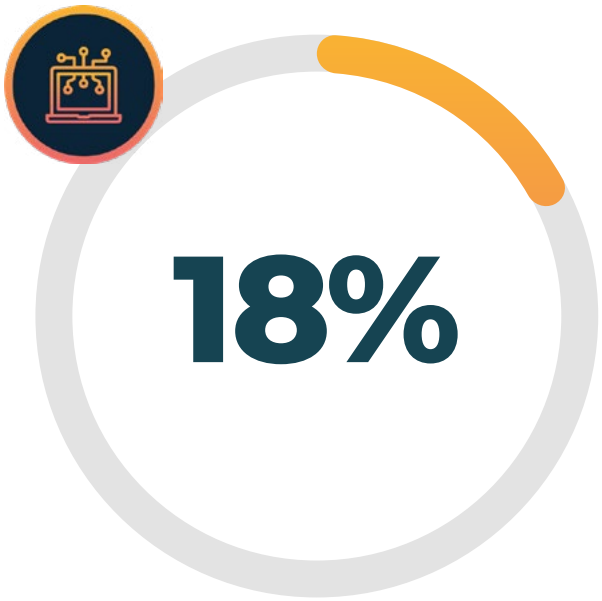
High on the agenda was anticipating attacks, with 48% saying they have undertaken a security risk assessment this year, and the same percentage have put a cyber policy in place to protect themselves financially in the event of a breach. Additionally, 39% have developed a formal incident response for dealing with ransomware attacks.

Supply chain risks is a huge topic of conversations within the cyber security community and so it was suprising to see that only 45% of those polled have a system in place to review security risks posted by immediate suppliers.

There are concerns for some companies about the systems they have in place to manage emerging threats. For example, 21% told us their cyber strategy is outdated and urgently needs to be refreshed to respond to new threats such as AI.

Security leaders are also hiring fresh cyber talent into the workforce. Of the security leaders surveyed, 42% told us that they have a fellow dedicated member of staff with cyber security as a formal part of their job role at their business.

However, successful attacks remain a regular occurrence. In total, 20% claimed their business was potentially compromised this year by a cyber breach. Meanwhile, 18% admit their business has suffered a serious cyber breach this year.



ADMIT THEIR BUSINESS HAS SUFFERED A SERIOUS CYBER BREACH THIS YEAR

PART 2: ADDRESSING THE AI THREAT

The are many reasons to be excited about the arrival of AI, but there are also substantial security issues.

Our survey revealed that 80% of security leaders feel that AI is the biggest cyber threat to their business. Meanwhile, 22% of respondents have chosen to ban staff from using AI chatbots like ChatGPT due to security concerns.

Interestingly, **research from the UK government** has shown that of those businesses currently using or planning to use one of the specified AI applications, the most common reasons for doing so were improving cyber security (35%) and creating efficiencies (35%).

Cyber concerns are also slowing down the pace of AI adoption. 76% told us that their AI implementation has been halted due to cyber risk. Whereas 81% claim the risks of AI are more of a threat than the benefits it brings.

Despite these issues, only 11% feel their organisation does not have robust cyber security measures to protect against AI-powered attacks in contrast to 89% who are confident.

OF SECURITY LEADERS FEEL THAT AI IS THE BIGGEST CYBER THREAT TO THEIR BUSINESS

PART 3: THE ROAD AHEAD

It's clear from our research that AI is a complex topic triggering a mixed reaction from cyber professionals. On the one hand, it can save time, money and contribute to the fight against external threats, on the other it can be a source of risk, data leakage and a compliance headache.

Our survey paints a worrying picture of the role AI is set to play in cyber crime in the future. 85% of respondents told us that AI advancements will outpace cyber defences. In preparation for this threat, 64% have seen an increase in their cyber budget this year, 27% have had their budget stay the same, and 7% have seen a decrease in budget.

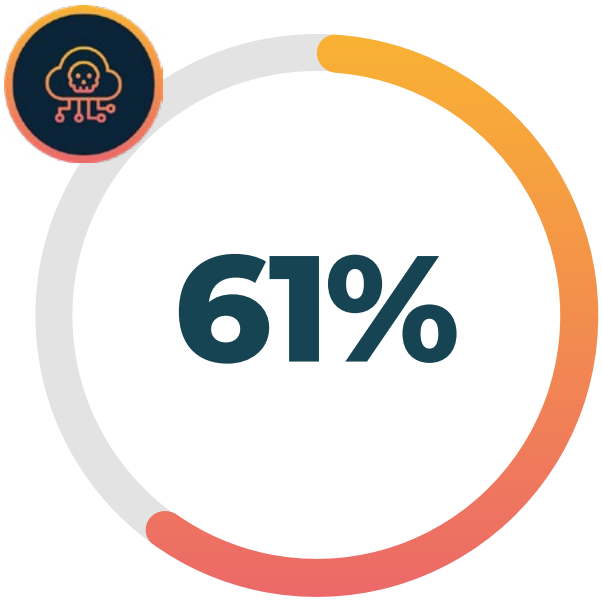
The rising volume and sophistication of attacks is also a key issue facing businesses. 61% have seen an increase in cyber-attack complexity due to AI, 33% have seen little change and just 4% have seen a decrease.

There have been growing calls for increased regulation of AI, from the United Nations Secretary General to the UK Prime Minister.

When asked about the role regulation should play in the management of AI, 95% agree that AI regulations are necessary in relation to cyber security, and 5% disagree.

Companies are also heavily increasing investment in processes and cyber defences. 69% are investing more in cyber protections against AI, 24% are keeping budgets the same, and 5% are decreasing spending.

However, the threat of a breach continues to worry cyber leaders. 63% expect a rise in data loss within their organisation this year, compared with just 32% expecting no change and 5% expecting a reduction in data loss.



HAVE SEEN AN INCREASE IN CYBER-ATTACK COMPLEXITY DUE TO AI

Nearly 40% of businesses reported a cyber attack in 2022 and we know digitally-enabled crime accounts for more than half of all offences.

There are clear benefits to AI but that cannot come without proper checks and balances and a legal framework to protect businesses and the economy.

It is vital that government, policing, security services and business work together to boost prevention, education, and protection in what is a rapidly developing industry.

Matthew Scott

Police and Crime Commissioner, Kent

CONCLUSIONS AND RECOMMENDATIONS

AI will continue to play a central role in discussions among government and regulators, but businesses must always look forward to how they can maximise AI technology while mitigating the risks.

Here are our top three recommendations based on the research:

1. **Embrace AI and don't let it hold back your business** – AI is here to stay, and businesses must understand that and dedicate resources to it. Whether it be bolstering cyber defences, driving efficiencies and boosting staff productivity or developing security strategies to protect against AI-powered threats, investment and learning in this area is essential for businesses moving forward.

2. **Ensure cyber security is a priority** – Even despite economic uncertainty, skills shortages and other barriers, cyber security should always remain a priority for businesses because attacks can hit any company regardless of size or sector. The financial, reputational and legal damage of cyber-attacks is devastating so security strategies can never be an afterthought. Upskilling employees, creating automation through AI, and outsourcing can provide businesses with the ability to maintain a strong security posture.

3. **Train staff to make AI work for them** – Training a roster of AI experts will enable businesses to embrace AI and ensure security remains a priority, while empowering staff to stay on top of developments and innovations. This can strengthen the power of AI by enhancing overall productivity while also stemming automation anxiety as AI can work hand in hand with staff. If AI is set to outpace cyber defences, then businesses need skilled staff to guide how AI is developed and deployed.

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