ABSOLUTE®

2024 ABSOLUTE SECURITY UNITED KINGDOM CYBER RESILIENCE REPORT

A Look at Cyber Resilience and Security Across the United Kingdom

Introduction

In an increasingly complex and dangerous world, cyber security remains at the very top of the agenda for boardrooms and CISOs alike, and rightly so.

From FTSE 100 listed companies to ambitious startups, no organisation is immune to growing volumes of increasingly sophisticated attacks.

Recent research from the UK government's **Cyber Security Breaches Survey 2024** revealed that such attacks are far more frequent than initially feared.

Half of UK companies (50%) and a third of charities (32%) report having experienced some form of cyber security breach or attack in the last year. The data showed that this figure rose dramatically when it came to medium businesses (70%), large businesses (74%) and high-income charities with £500,000 or more in annual income (66%).

Phishing scams designed to breach endpoint security remain the most common cause of attack, with 84% of businesses and 83% of charities citing it.

The cost of such breaches is immeasurable, from reputational damage and a loss of customer trust to recovery bills worth hundreds of thousands of pounds.

Worse still, the widespread use of Artificial Intelligence (AI) is a powerful tool in the hacker's arsenal of weapons, allowing them to deploy high-impact attacks with devastating ease.

With British businesses facing a new wave of hostile security threats, Absolute has set out to examine the challenges facing Chief Information Security Officers (CISOs), in terms of cyber resilience, AI and emerging threats.

This report will shine a spotlight on how security leaders plan to meet these challenges, as well as provide insight, analysis and guidance for CISOs tasked with managing this threat.

Methodology

Absolute commissioned polling of 250 UK-based Chief Information Security Officers (CISOs) in May 2024. The research was conducted by independent polling agency Censuswide and included respondents from enterprise businesses.

PART ONE:
Cyber resilience in a dangerous world

As high-profile cyber attacks on government infrastructure and large businesses continue to dominate the news agenda, having resilient cyber defences in place remains a top priority for security leaders. Absolute defines Cyber Resilience as a paradigm larger and more critical than traditional cybersecurity, as it not only ensures defences are working as intended, but also helps organisations withstand and quickly recover from cyber disruptions and attacks.

Our research revealed that 91% of CISOs believe cyber resilience is more critical for their organisations than traditional cybersecurity. This figure underlines the increasing need for security systems with effective defences and recovery capabilities, against the backdrop of increasingly regular attacks.

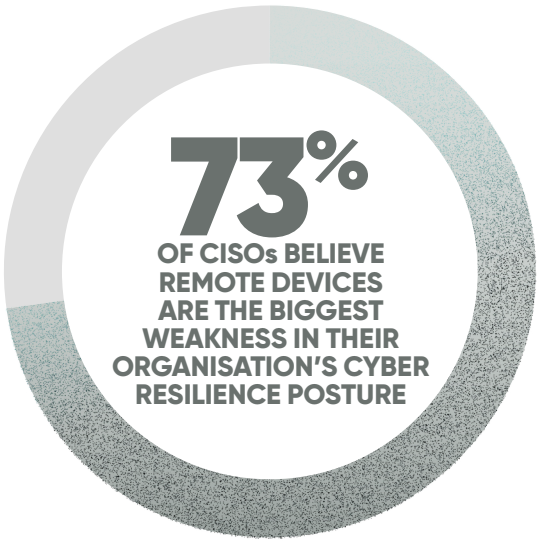
When it comes to cyber readiness, an impressive 97% of respondents told us they have a dedicated cyber resilience strategy in place, with the same number claiming they have a well-defined incident response protocol.

An increase in the reliance of automation to bolster cyber defences was also evident. Ninety-Six per cent of those surveyed told us that they had invested in automation technology to improve cyber resilience.

The data also revealed that CISOs regularly review their protocols, with 94% saying they update their cyber resilience strategy more than once a year. However, the impact of rampant inflation and high interest rates is beginning to take its toll. In total, 45% claimed they have had their cybersecurity budget slashed due to economic uncertainty over the past year.

In terms of skills and training, CISOs were making huge progress when it comes to educating fellow board members about the extent of cyber risk. Ninety-three per cent of respondents told us that their C-Suite had been sent on cyber resilience training courses.

When it comes to the reasons why organisations are choosing to invest in cyber resilience, 89% said that they feel that mitigating financial loss is the biggest driver behind improving cyber resilience. However, 43% admit that their cybersecurity team haven't been given enough budget to keep their organisation protected.



In terms of threats, 94% of CISOs said they are prioritising preventing cyber threats over recovering from them. However, flexible working remains a serious challenge, with 72% claiming remote working has complicated their organisation's cyber resilience posture. Additionally, 73% believe remote devices are the biggest weakness in their organisation's cyber resilience posture.

Confidence in security capabilities remains low however, with 77% saying they believe that the UK is falling behind the US and EU when it comes to national cyber policies. A further 64% say the UK has a poor cyber resilience strategy.

Despite huge economic challenges, 85% say that cyber is the biggest threat facing the UK right now.

PART TWO:

The Emerging AI Threat

Artificial Intelligence (AI) technology is already shaking up traditional working models, bringing with it opportunities but also huge challenges.

Interestingly, 46% of respondents told us that AI is more of a threat to their organisation's cyber resilience than a benefit. Worryingly, 54% feel their organisation's security team is unprepared for evolving AI-powered threats.

It's not all bad news however, as 77% say they believe that AI has filled the cybersecurity skills gap, bringing additional cost-saving benefits to the senior team. Against this backdrop, it is encouraging to see that 83% of those surveyed say they have prioritised hiring AI experts over the past year.

Concerns and mistrust over risk remain high though, with 39% of CISOs having personally stopped using AI due to fears of a cyber breach.

A notable portion of security chiefs have also taken a hardline approach to AI adoption in the workplace. For example, 44% have banned AI used by employees at their organisation due to fears of a cyber breach.

In preparation for using the technology ethically and responsibly, 85% said their C-Suite has been sent on AI training courses.

On a national scale, however, there is concern that the technology is not being fully embraced, with 68% saying they believe the UK isn't advancing its AI development quickly enough.

PART THREE:
Threats Ahead

With growing volumes of increasingly sophisticated attacks leaving security leaders under pressure, we also explored attitudes towards threat mitigation and cyber planning.

A shocking 47% of those surveyed said their organisation have been attacked by an increasing number of state-sponsored attacks over the past year. Meanwhile, 62% said they are worried they could lose their job if their organisation was hit by a major successful cyber attack.

In terms of specific threats, 48% said their organisation was hit by a ransomware attack in the past year. An additional 69% said the financial loss from a successful ransomware attack could cripple their organisation.

Eight in ten CISOs told us that ransomware was their organisation's biggest cyber concern currently.

Perhaps most shockingly, over one-third (35%) admitted to ignoring the National Cyber Security Centre's (NCSC's) cyber guidance.

48%
SAID THEIR ORGANISATION WAS HIT BY A **RANSOMWARE ATTACK** IN THE PAST YEAR.

8 IN 10
CISOs TOLD US THAT RANSOMWARE WAS THEIR ORGANISATION'S BIGGEST CYBER CONCERN CURRENTLY

Conclusion

In conclusion, our report has helped to shine a spotlight on the challenges facing CISOs in an increasingly dangerous world. We have established that cyber security and specifically cyber resilience remain top priorities in the boardroom.

In support of this strategy, it is clear that security leaders are doing their best to ensure fellow C-suite colleagues are equipped with the latest cyber and AI training.

However, budget cuts remain a problem, leaving CISOs hamstrung with limited funding despite rising threats. The relationship with the NCSC is also a problem, with a disconnect between the guidance offered and the rules followed.

Overall, we are pleased to report that CISOs have a clear understanding of the critical role cyber resilience can play in the safety and security of their organisation, both now and in the future. However, many still find themselves under pressure to use AI to drive operational efficiencies yet recognise that the technology is open to misuse and could pose a major security risk.

/ABSOLUTE®

Absolute Security is partnered with more than 28 of the world's leading endpoint device manufacturers, embedded in the firmware of 600 million devices, trusted by 21,000 global enterprises, and licensed across 14 million PC users. With the Absolute Security Cyber Resilience Platform integrated into their digital enterprise, customers ensure their mobile and hybrid workforces connect securely and seamlessly from anywhere in the world and that business operations recover quickly following cyber disruptions and attacks. Our award-winning capabilities have earned recognition and leadership status across multiple technology categories, including Zero Trust Network Access (ZTNA), Endpoint Security, Security Services Edge (SSE), Firmware-Embedded Persistence, Automated Security Control Assessment (ASCA), and Zero Trust Platforms.

Contact Us