

The logo for SRM, featuring the letters 'S', 'R', and 'M' in a bold, white, sans-serif font. A small orange triangle is positioned between the 'S' and 'R'.

2023

Cyber Security Insights Report



Contents

	Introduction	3
	At a glance	4
01	Cyber budgets barely move	5
	<i>Focus on people: A people problem?</i>	10
02	How industry sectors influence incident experience	11
	<i>Focus on people: Does 'who' really matter?</i>	13
03	Top cyber security challenges	15
	<i>Focus on technology: AI amplifying threat actor tactics, techniques and procedures</i>	17
	<i>Focus on technology: Areas of cyber security enhanced by AI</i>	18
	Contributors	20

The top half of the page features a composite background. On the left, there are vibrant, glowing blue and purple microscopic cells, possibly bacteria or neurons, with a textured, bubbly appearance. On the right, a series of vertical grey bars of varying heights, resembling a bar chart, are set against a dark background. A faint silhouette of a person is visible behind the bars, suggesting a human element in data analysis or technology.

Introduction

The **S-RM Cyber Security Insights Report 2023** reflects the cyber security experiences of 600 C-Suite and senior IT professionals within large organisations over the past year¹. We asked this audience about their most pressing cyber challenges, their experience of cyber security incidents, and their cyber budgets, so you can make better-informed decisions about your own security.

This year, cyber security budgets rose slightly but this muted increase, in the face of an increasing threat, suggests a greater focus on getting value from existing resources. Our data indicates that while investing in the right technology solutions remains a high priority, there is increasing recognition that getting the right people and governance in place is as crucial to maximising the return on those investments. Although our research also indicates that C-Suite leaders and IT professionals may not always agree on this.

Serious cyber incidents continue to occur across all sectors and the average direct costs relating to one incident increased 11% YoY to USD 1.7 million. This year, we explored how industry sector and size can inform likely attack vectors and incident costs, and how those insights can influence your security programme.

But among new developments, some things have remained consistent. Hybrid working and a lack of organisational cyber awareness continue to be the main security challenges faced by our respondents. We analyse how some of the past years' developments in AI may exacerbate or alleviate these concerns. We hope our findings offer support and guidance as you plan your approach to cyber security in the coming year.

¹ Survey commissioned by S-RM and conducted by market research firm Vanson Bourne in September 2023. Survey consisted of 600 C-Suite and IT budget holders from organisations in the UK and US with a revenue over USD 500m.

Findings at a glance

11%

INCREASE IN DIRECT
COST OF A SERIOUS
INCIDENT

The average direct cost of a single serious cyber incident has risen.

63%

EXPERIENCED A
SERIOUS INCIDENT IN
THE PAST 3 YEARS

Serious cyber incidents continue to occur across all sectors.

3%

AMOUNT CYBER
BUDGETS INCREASED
IN 2023

Cyber budgets have had a muted increase this year.

97%

PLAN TO INCREASE
THEIR USE OF AI-BASED
TECHNOLOGIES IN THE
NEXT 12 MONTHS

But only 53% are confident they can secure the use of AI across the business.



01

Cyber budgets barely move

Cyber security budgets increased for the third consecutive year but remain below expected spend in 2022. Priorities are shifting when it comes to 'value for money' as organisations optimise their spending with little room to manoeuvre.

In 2023, the average cyber budget for a large organisation rose by 3% year-on-year to USD 27.1 million (figure 1). This muted increase has again fallen short of the expectations of senior IT professionals and their C-Suites (figure 2). Since 2021, our respondents have consistently overestimated their anticipated budget for the subsequent 12-month period. Although budget owners predict an 8% increase for 2024, the funding available to security decision-makers is unlikely to be as generous.

Looking across geographies, budget growth in the US slowed to 1%, falling almost in line with the UK in absolute terms after outstripping it in 2022 (figure 3).

FIGURE 1
Average cyber security budget (USD million)

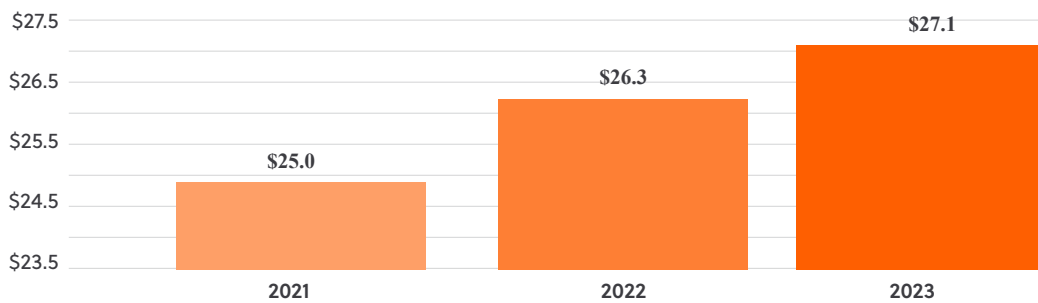


FIGURE 2
Actual vs predicted budget increases

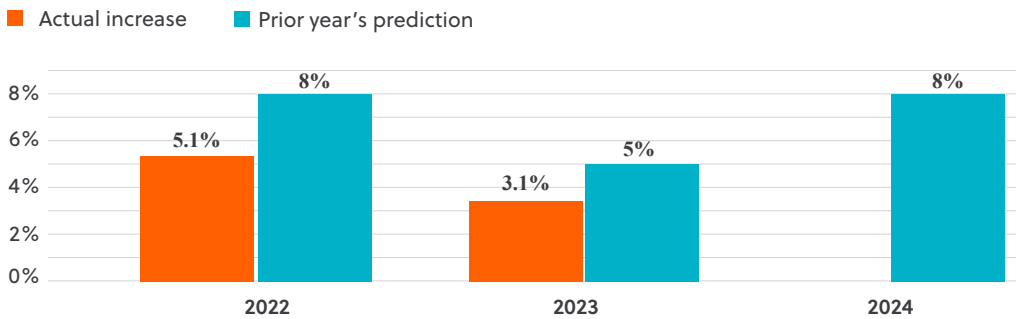
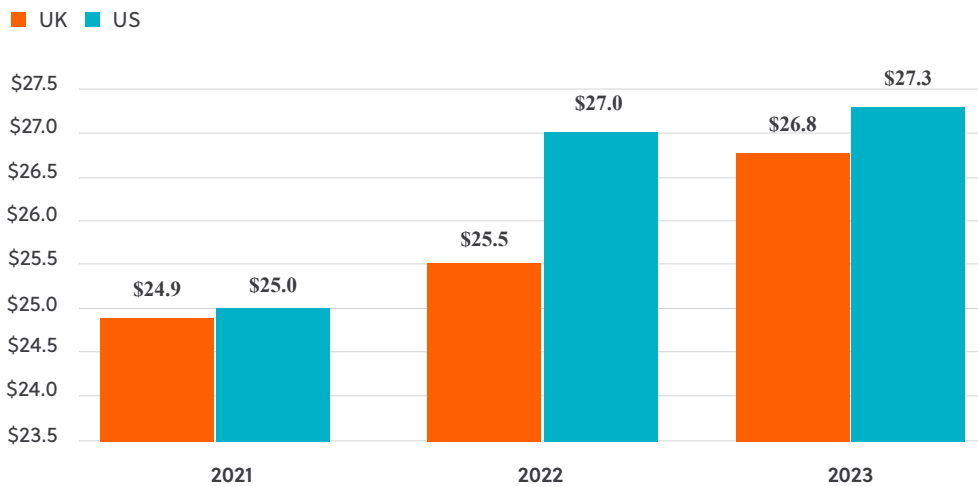


FIGURE 3

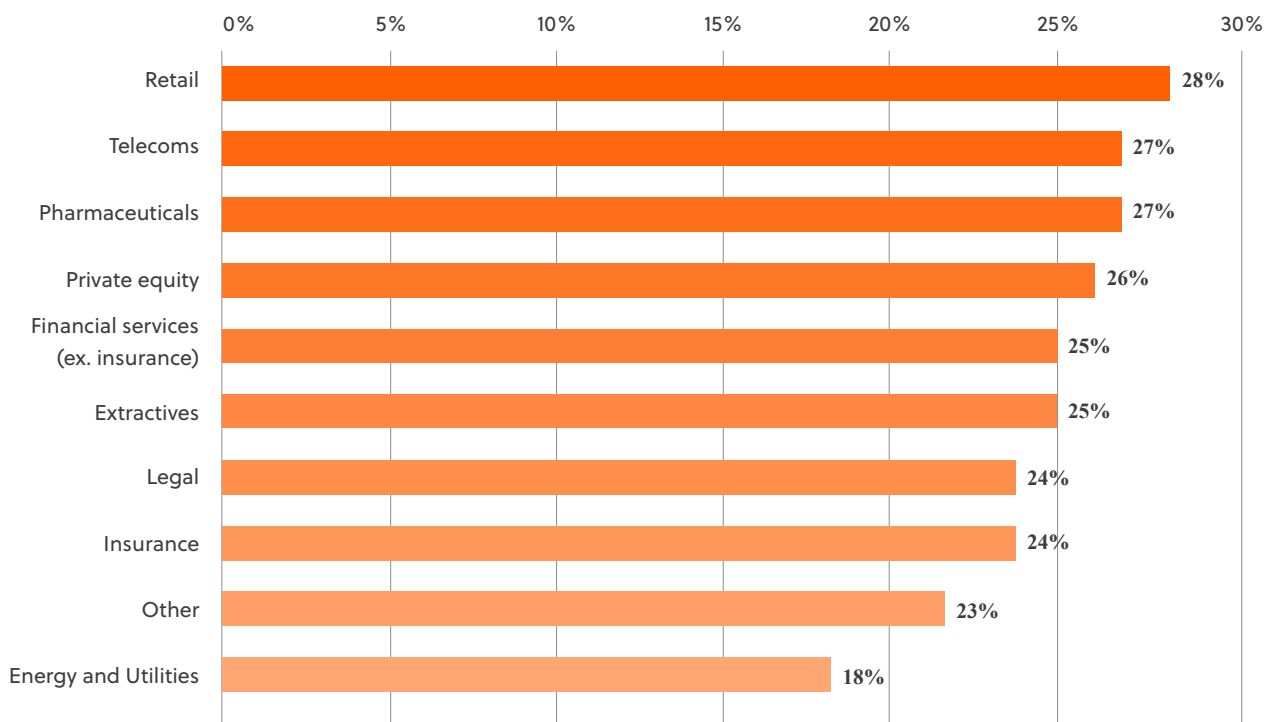
Average cyber security budgets - UK vs US (USD million)



When it comes to cyber budgets as a percentage of an organisation's overall IT budget, the UK and US remained aligned, allocating approximately 24% and 25% of IT budgets to cyber respectively. While marginally lower than 2022's overall average (26%), this consistency demonstrates an ongoing commitment to cyber security, and is reflected across almost all sectors (figure 4). Only the Energy and Utilities segment stands out as underinvesting in security from a proportional budget allocation perspective.

FIGURE 4

Percentage of IT budgets allocated to cyber security



Finding value for money

Over the past three years, we have consistently been told by respondents that ‘investment in technology’ represents the highest value for money. While that remains the case in 2023 (table 1), this enthusiasm seems to be waning (figure 5).

TABLE 1

Top 5 investment areas delivering ‘high value for money’






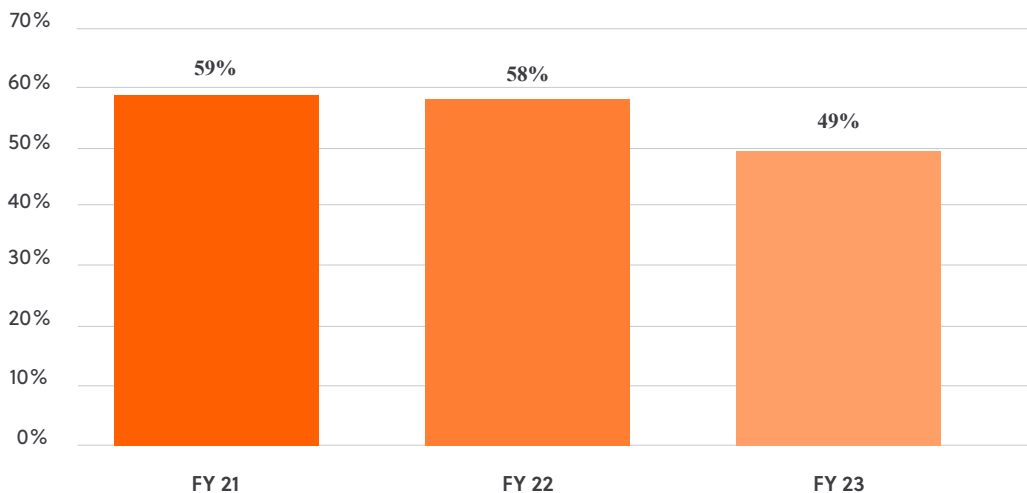
				
Cyber security technologies	Threat intelligence	Risk assessments	Cyber insurance	Third party risk management
49%	46%	42%	42%	40%

FIGURE 5

Percentage of respondents citing investment in technology as ‘high value for money’



The dip likely reflects a growing awareness that investing in cyber security technology also means investing in the governance and personnel to effectively enable and manage it. This view seems more prevalent among the IT professionals charged with implementing these solutions than their C-Suites.

Only 43% of IT professionals cited technology as a ‘high value for money’ investment area, compared to 56% of C-Suite business leaders (table 2). The difference perhaps reflects a misalignment of expectations between the operators of cyber technologies, and those a step removed from their day-to-day applications.

TABLE 2

Investment areas considered 'high value for money' by respondent role

	IT/Cyber budget holders	C-Suite/Senior business decision makers
Cyber security technology	43%	56%
Cyber insurance	36%	48%

We found a further dislocation in attitudes to cyber insurance. C-Suite business leaders see greater value for money than IT professionals in having a cyber security insurance policy in place (48% versus 36%). This is perhaps because C-Suites are impacted by the business interruption, regulatory and reputational implications of a cyber incident beyond the immediate effects on the IT estate. They will also rely on insurance to mitigate more than just the costs associated with the remediation of technical infrastructure.

When budgets are tight, we see organisations taking three broad approaches to managing cyber risk:

1 IT and security optimisation: Identifying cost reduction opportunities by making existing processes more efficient to free up budget for more costly or labour-intensive IT and security initiatives. For example, undertaking a technology benefit analysis exercise to determine whether using multiple solutions and vendors for risk reduction is preferential to security capabilities delivered by a major cloud provider under one roof.

2 Future-focused investment: Investing now in security initiatives for long-term cost savings. Examples include establishing cross-functional security governance programmes, adopting AI and automation, and focusing on prevention and early identification of cyber attacks.

3 Outsourcing: Contracting out IT and security functions to managed service security providers (MSSP) or virtual CISOs (vCISOs).



FOCUS ON PEOPLE

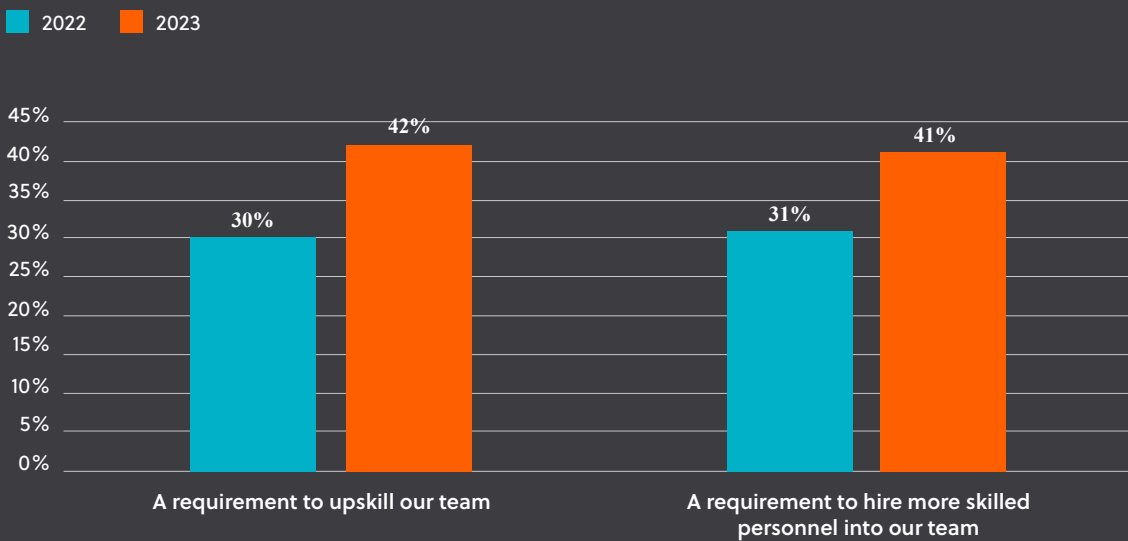
A people problem?

Our respondents expect talent development and acquisition to be greater drivers of future increases in budgets than in 2022 (figure 6).

The challenge of recruiting and retaining skilled security professionals has been well-documented. Rising demand for cyber talent has met a deficit in supply, creating rising competition for staff and a variety of skills gaps in the labour market.

This skills shortage is compounded by two key factors. Ambiguity still surrounds cyber security as a profession, hindering those who might be ready for a cyber career from entering the jobs market. Inflated job requirements for entry level positions have also hindered talented professionals from building cyber careers. Security leaders who are more open to diversifying their talent pools stand to benefit.

FIGURE 6
Reasons for anticipating increased cyber budget next year





02

How industry sectors influence incident experience

Serious cyber incidents continue to occur across all sectors with increasing direct costs. Attack and impact types vary according to sector, which can help to inform cyber risk management.

Nearly two thirds (63%) of organisations experienced a serious cyber incident within the past three years. The direct costs relating to a cyber incident increased by 11% year-on-year to an average of USD 1.7 million in 2023.

Variance across sectors

The top three most commonly cited attack types experienced were 'fraud' (e.g. payment misdirection), 'third party related compromise' and 'data exfiltration'. While most cyber attacks are indiscriminate, it is useful to analyse the variation in attack types across sectors as it can prove helpful for risk managers (table 3).

TABLE 3

Attack by sector type

Sector	Most common attack type	%
Legal	Cryptojacking (i.e. unauthorised crypto mining)	35%
Insurance	Data exfiltration	34%
Private equity	Ransomware/extortion	57%
Extractives	Third party related compromise	50%
Financial services (ex. Insurance)	Data exfiltration	46%
Retail	Third party related compromise	41%
Telecoms	Hactivism/website/social media defacement	49%
Pharmaceuticals	Hactivism/website/social media defacement	61%
Energy and Utilities	Third party related compromise/denial of services/sabotage	33%
Other	Fraud (e.g. payment misdirection)	42%



Financial services: These firms are attractive targets for data exfiltration given the high-sensitivity data they hold. Beyond the regulatory costs associated with data loss, the risk of losing customer trust is higher than average. Of all sectors, financial services cited 'Reputational Damage' most frequently (44%) as an impact of a cyber attack.



Retail, Extractives, and Energy and Utilities: Respondents from these sectors all cited third party related compromise as one of their most frequently experienced attacks (41%, 50% and 33% respectively). This reflects their interconnected operational landscape, and has been high on the agenda of Chief Risk Officers for the last three years, following high profile attacks targeting the likes of SolarWinds (2020), Kaseya (2021) and MOVEit (2023).



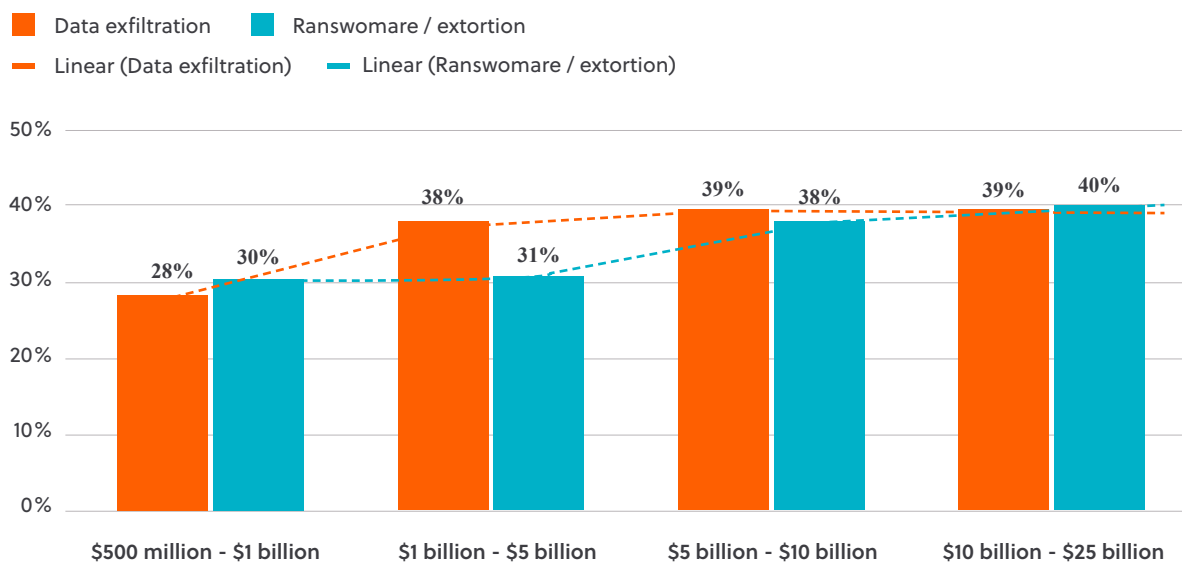
Pharmaceuticals: 61% of these firms reported hactivism as their most common attack type. Pharmaceutical firms face relatively high levels of public scrutiny, making them greater targets for hactivist groups with socio-political agendas.

Heightened risks for larger firms

The bigger the organisation, the greater the risk of experiencing a data exfiltration and ransomware attack (figure 7). Larger organisations are more likely to hold greater volumes of sensitive data, and often have broader operational footprints which are harder to govern consistently.

FIGURE 7

Percentage of organisations that experienced data exfiltration and ransomware/ extortion attacks by revenue (USD)



FOCUS ON PEOPLE

Does 'who' matter?

When it comes to building resilience against cyber attacks, understanding who is attacking you can matter less than understanding the most common tactics, techniques and procedures that threat actors collectively use.

Although targeted attacks occur, most victims are compromised because they present easily exploited vulnerabilities for more indiscriminate attacks, which threat actors cast over a wide surface area. Building cyber resilience is more an exercise in understanding the threat actor ecosystem as opposed to understanding the nuanced differences between groups.

However, during an incident, detailed threat intelligence about who has targeted you is critical to devising a coherent and effective response strategy. This includes insights into what type of pressure tactics the group may use against you, the ransom amounts they may demand and, should you choose to engage with them, how reliable they are in negotiations.

Impacts and costs

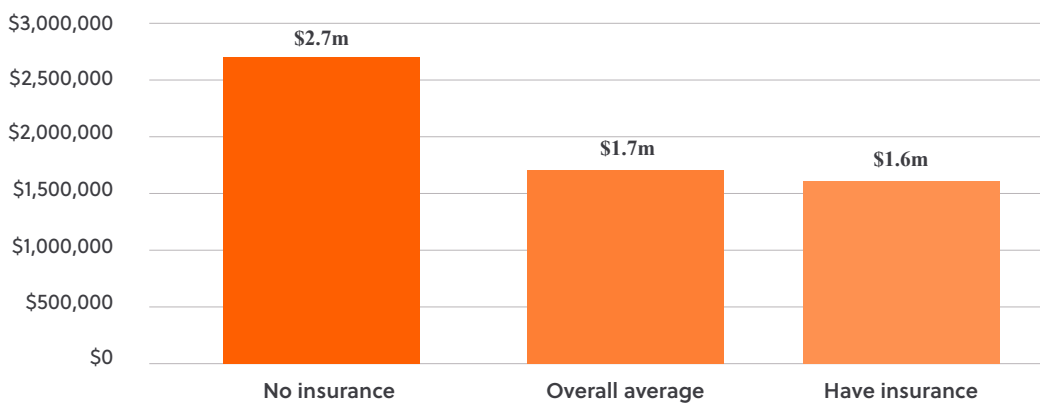
The top three impacts of a cyber attack on our respondents were increased insurance premiums (37%), operational downtime (36%) and recovery/response costs (32%). The average direct costs associated with these impacts was USD 1.7 million per incident, however in the extractives sector, these costs were almost 80% higher than average, standing at USD 3 million.

When we analyse the types of impact experienced by the extractives sector, we see that respondents from extractives firms cited operational downtime most frequently (50%). Cyber attacks that specifically target operational technology remain rare. However, should these systems become unavailable, the impact can be significant and occasionally lead to costly operational disruption.

We saw another clear trend in the relationship between insurance and incident costs (figure 8). Costs in 2023 were substantially higher for those organisations who did not have cyber insurance, averaging almost USD 2.7 million per incident (60% above average and 70% higher than insurance holders). In terms of the 'high value for money' C-Suite and senior leadership place on insurance, the investment appears to be worth it.

FIGURE 8

Average direct costs of a single cyber incident USD million





03

Top cyber security challenges

The largest companies continue to find that their greatest cyber security challenges relate to their people – where they work, and how they respond to cyber threats. This year's breakout AI technologies have the potential to further exacerbate this.

Respondents told us their top two cyber security challenges are 'hybrid working' and 'lack of understanding around cyber trends and threats' (figure 9). Although the prominence of hybrid work as a security challenge has diminished since 2021 (figure 10), it remains a persistent issue as global working patterns settle on various hybrid permutations. People remain at the heart of cyber security, and hybrid working presents unique challenges in maintaining visibility of an organisation's attack surface and ingraining a cyber-first culture amongst staff.

The issue goes hand-in-hand with the second-most cited challenge area: 'lack of understanding around cyber trends and threats'. This corresponds with the fact that 'maintaining security against evolving cyber threats' was the most cited reason for anticipated future rises in budgets.

FIGURE 9
Main cyber security challenges for organisations in 2023

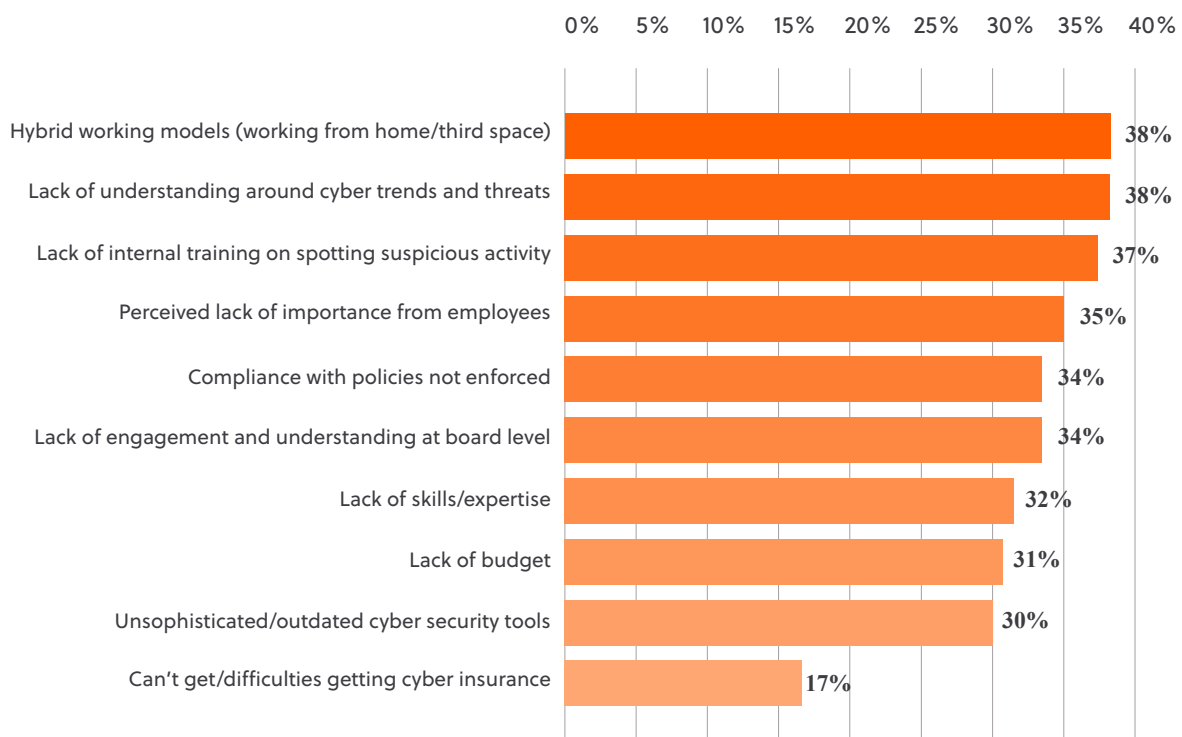
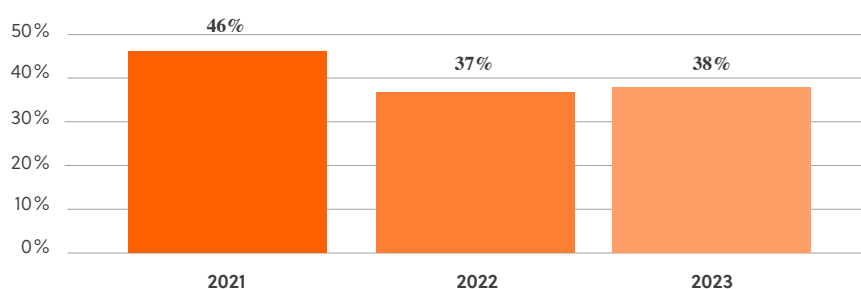


FIGURE 10
Percentage of respondents citing 'hybrid working models' as a cyber security challenge



FOCUS ON TECHNOLOGY

AI amplifying threat actor tactics, techniques and procedures

AI provides threat actors with a resource that can work across multiple tasks simultaneously with no downtime. Given the repetitive tasks involved in phishing campaigns, the deployment of AI across a range of these tasks is inevitable.



Targeted spear phishing

It is very time consuming for a human to scrape public data, identify people who have recently joined a company, and design and send a fake email from the company's IT team containing a malicious link. AI could feasibly do this every day, messaging thousands of people at once with custom attacks.



Ongoing correspondence

In many cases, the more effort a threat actor spends corresponding with a victim, the bigger the potential payoff. We see this with invoice fraud attacks, where threat actors

will go to great lengths to convince someone that they are a legitimate business which has simply changed their bank account details. But a single threat actor can only handle so many conversations at once. An AI could handle multiple conversations simultaneously without getting confused or distracted.



Rise of vishing

Voice emulation is getting better every day. It is currently not possible to emulate someone's voice in real time on consumer hardware, but it will not be long until this is the case. When that happens, phone calls will become a more lucrative platform for threat actors. An AI would be capable of having multiple conversations with victims at once – similar to how commercial call centres are currently experimenting with the same technology.

In terms of evolving cyber threats, we are likely to see a surge of AI-enabled or amplified social engineering attacks, and raising awareness amongst staff and security teams about this will become more important. Half our survey respondents say that they are still understanding / studying the threat of AI, and they may have to catch up fast.

But AI will not only be a force multiplier for threat actors, it also presents some compelling opportunities for businesses to better protect themselves. AI can simplify historically complex tasks, aiding security teams in a range of ways including automated script creation for expedited data scrutiny, seamless reporting, and integration with Security Orchestration, Automation and Response (SOAR) platforms. AI-driven advancements in Endpoint Detection and Response (EDR) are also ushering in significant enhancements. The integration of generative AI within SIEM platforms, such as Microsoft Security CoPilot, is poised to make a transformative impact on security measures.

FOCUS ON TECHNOLOGY

Areas of cyber security enhanced by AI

There are a number of areas where AI is likely to enhance cyber security capabilities, variously offering greater speed, accuracy and/or cost-effectiveness:



Real-time threat detection

AI's ability to scan extensive data volumes in real-time revolutionises threat detection and response. While traditional SOAR platforms have struggled with large-scale event categorisation and disproportionate responses, AI demonstrates potential in addressing these issues and reducing the time required for incident detection.



Automated response

AI can play a pivotal role in automating threat responses. It facilitates large-scale evidence collection and analysis, pinpointing anomalies, and guiding investigators on where to start their investigation. Triage artifact collection and parsing become streamlined, saving time and resources, and rapid remediation becomes possible with enough foresight and planning.



Predictive analysis

The ability of AI to employ predictive analysis is not just an incremental step forward but a potentially ground-breaking leap in cyber security. In contrast to traditional reactive security measures, by analysing existing patterns, AI can forecast potential threats even before they manifest. AI may also mean organisations can not only identify but also understand the evolution of these threats, enabling greater preventative measures, and more efficient allocation of security resources.



Automated risk and compliance

Instead of periodic compliance reviews, which might leave vulnerabilities exposed for extended periods, AI can constantly monitor systems and processes, flagging any deviations immediately.

AI also changes nothing about the threat vector itself. Existing controls – such as spam filters, training and awareness, MFA, EDR, etc – are still the best defence against any intrusion. We are likely to see higher volumes and more targeted attacks, but by developing strong governance and implementing basic security controls, organisations will already be ahead of the curve.

Almost all (97%) of our survey respondents said they were looking to increase their use of AI-based technologies (outside of IT/ IT security) over the next 12 months. The use of large language models (LLMs) such as Chat-GPT and its equivalents will likely be most prevalent. However, only 53% of those respondents said they were completely confident in their security function's ability to secure the use of AI across the business. Their concerns likely relate to:

- **Data privacy:** The risk of AI accessing or leaking sensitive data without robust governance.
- **Reliability:** Ensuring AI's dependability in threat detection without misinterpretations of vital information.
- **Complexity:** The expertise required to implement AI and cyber solutions successfully and securely.

This era marks a significant juncture for cyber security innovation. Both threat actors and their targets know they will have to invest in the latest technologies, and the best talent, to achieve their objectives.



Contributors

Casey O'Brien

DIRECTOR OF OPERATIONS, CYBER SECURITY

Gideon Teerenstra

HEAD OF CYBER ADVISORY, BENELUX

Harriet Martin

ASSOCIATE DIRECTOR, CYBER SECURITY

Jamie Smith

BOARD DIRECTOR, GLOBAL HEAD OF CYBER SECURITY SERVICES

James Jackson

ASSOCIATE DIRECTOR, CYBER SECURITY

Joani Green

TECHNICAL DIRECTOR, CYBER SECURITY

Katherine Kearns

HEAD OF PROACTIVE CYBER SERVICES, EMEA

Lenoy Barkai

DIRECTOR, CYBER SECURITY

Michael Clark

HEAD OF CYBER ADVISORY, AMERICAS

Contact us

To discuss how we can help support any aspect of your cyber security, please reach out to

Jamie Smith, Board Director, Global Head of Cyber Security Services | London, j.smith@s-rminform.com

Paul Caron, Head of Cyber Security, Americas | New York, p.caron@s-rminform.com

Martijn Hoogesteger, Head of Cyber Security, Benelux | Utrecht, m.hoogesteger@s-rminform.com

S-RM is a corporate intelligence and cyber security consultancy. We provide intelligence, resilience and response solutions to organisations worldwide.

Founded in 2005, we have 400+ experts across ten international offices, serving clients across all regions and major sectors.

