78 St Vincent Street
Glasgow G2 5UB
t: 0141 370 9919
e: info@be-it.co.uk
w: www.be-it.co.uk

Cyber Security Study

Comprehensive Survey Report

Introduction

Cybercriminals today operate like highly organised enterprises—complete with recruitment strategies, performance targets, and sophisticated tools designed to stay ahead of defenders.

As a UK Government Head of Cyber Security once observed:
"The criminals are brilliant at what they do. They are professionally organised 'businesses', with sales targets, recruitment strategies and everything they need to try to stay one step ahead of our efforts to counter their activities."

The scale of the challenge is growing. According to the UK Government's 2024 Cyber Security Breaches Survey:

50% of businesses and 32% of charities reported a cyber breach or attack in the past year.

For medium businesses, this rises to 70%, and for large businesses, 74%.

Survey Link

Phishing remains the most common attack, affecting 84% of businesses and 83% of charities, followed by impersonation attempts (35% and 37%) and malware (17% and 14%).

The financial impact is significant. Government figures show the most disruptive breach cost businesses an average of £1,205, rising to £10,830 for medium and large firms. Charities faced an average cost of £460.

However, global research paints an even starker picture: IBM's Cost of a Data Breach Report 2024 estimates the average cost of a breach in the UK at £3.58 million, and globally at $4.88 million (≈£3.9 million)—with healthcare breaches exceeding $9.7 million.

These numbers underline a critical reality: cyber threats are pervasive, costly, and evolving. This survey aims to understand how organisations are responding—what measures they have in place, where gaps exist, and what support they need to strengthen their defences.

Executive Summary

The two biggest internal challenges for companies at present are:

- Budget constraints, mentioned by 67%
- Skills gap, mentioned by 61%

When we asked specifically if there are enough cyber security professionals in Scotland/UK, only 26% said 'yes', with 42% saying 'no' and 32% saying 'not sure.'

A general impression, supported by the data, is that some people and companies are outwardly more confident in their own organisation's anti-cyber-crime measures than those in other companies/their suppliers. We saw this in the fact that 36% were 'very confident' in their own organisation's ability to prevent cyber-attacks, with 41% being 'somewhat confident.' Similarly, 37% were very confident in their organisation's ability to recover from a cyber-attack, with 42% 'somewhat confident.'

However, when asked whether their customers are doing enough to prevent cyber-crime, only 31% said they are, with 38% saying they are not (and a further 31% undecided). Moreover, when asked about their company's supply chain, 45% said it was 'somewhat' or 'very' secure, but a majority (55%) said it was either 'averagely,' 'somewhat' or 'very' vulnerable. This seems to us to be a problem. While it's understandable that companies do not want to be seen to have had their security breached, it is important that they are honest about it when it happens, otherwise the true extent of the problem will be hard to ascertain accurately.

Companies' senior management do appear to be aware of the threats, with 39% saying their organisation's exec team is 'very involved' in their cyber security strategy and a further 44% saying they are 'somewhat involved.'

In general, the surveys showed that the public sector is perceived to be behind the private sector, with 57% saying the public sector is not doing enough to prevent cyber-attacks, compared to 46% of the private sector who said this.

More training to meet future needs. 60% said not enough people were being trained in cyber security generally. Given that hardly a day seems to go by without another story of another company suffering a cyber-attack, the lack of talented cyber security people at present and the lack of sufficient people coming through training means that Scotland/UK faces what is undoubtedly a growing threat.

The types of external support that would be most valuable to organisations were:

- Staff training and awareness (67% mentioned this)
- Compliance and audit support (57%)
- Cyber-security consulting (55%)
- MDR (managed detection and response) 49%

Another possible way for companies to mitigate skills challenges is to outsource cyber security to a third-party. However, our results suggest that while 10% already do and 25% would consider it, over a third (35%) would not do this.

When we then asked if it is acceptable to have cyber-security providers based overseas, a small majority (46%) said 'no,' while 41% said 'yes.'

71% believe future hires in this area will need to have stronger technical skills than today.

57% expect technology to 'somewhat replace or complement human judgment' in financial services crime decision-making.

AI was the most commonly cited important future resource for tackling cyber-crime.

Methodology

Once again, the survey was conducted thePotentMix on behalf of Be-IT Resourcing. thePotentMix is an extremely experienced recruitment, media and marketing company with an established track record in research work. We received nearly 200 responses from cyber security professionals and related jobs, both within Be-IT's database and also from others with established reputations whom we specifically targeted to take part.

The key findings of this year's study are shown in the Executive Summary below. The remainder of the report then considers each question in more detail. If you have any questions or comments, please get in touch with Christina Hall.

Recommendations

- Increase investment in cybersecurity training and awareness programs.
- Develop a clear strategy to address the skills gap through education and recruitment.
- Ensure regular testing of incident response plans.
- Strengthen third-party risk management and compliance monitoring.
- Promote executive involvement in cybersecurity strategy.
- Leverage AI and advanced technologies to enhance threat detection and response.

Introduction: general questions

Q. 1 Job title

There were 111 different job titles given, reflecting a broad range of the IT industry generally, but with the vast majority being involved in cyber security/data management/QA etc. A full list is attached in the Appendix.

Q. 2 Private, Public or Third Sector

- 81% of responses came from the Private sector
- 17% came from the Public sector
- 2% came from the Third sector

Q. 3 Sise of company/organisation

- 10% of responses came from start-ups of up to 10 employees
- 16% came from small (11-50 employees) companies
- 21% came from medium (51-250) companies
- 21% came from medium (51-250) companies
- 18% came from large (251-1,000) companies
- 35% came from very large (1,000+) companies

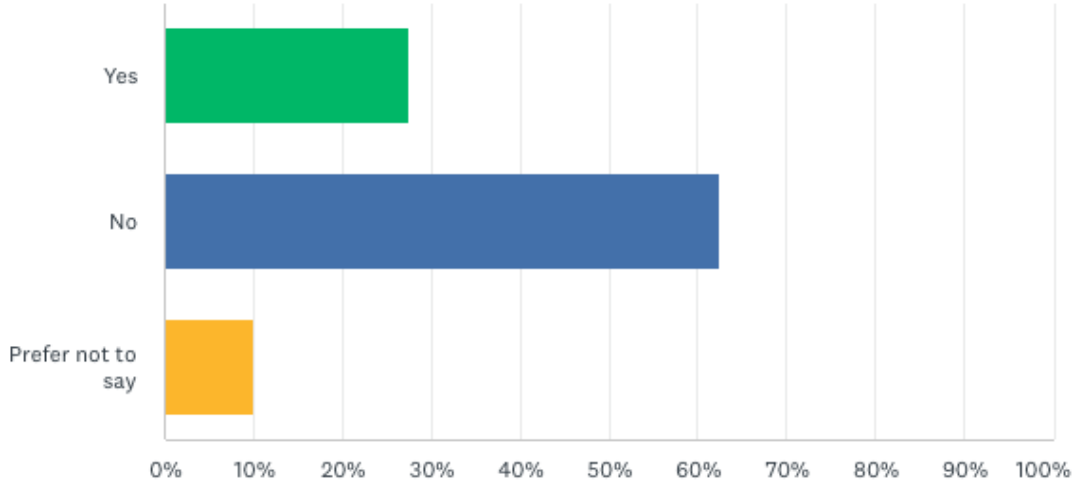
Q. 4 Location

- 55% were based in Central Scotland
- 4% were based in Northern Scotland
- 1% were based in Southern Scotland
- 6% were based in the North of England
- 4% were based in the English Midlands (including East Anglia)
- 25% were based in London/South East England
- 4% were based in South-west England
- 1% were based in Wales

Cyber Crime: are we doing enough?

Detailed, question by question analysis

Q. 1 Has your organisation experienced a cyber-attack in the last three years?



- 27% said yes
- 63% said no
- 10% didn't want to say if they had or not

At first glance, these figures suggest that most organisations have avoided cyber-attacks in recent years. However, this contrasts sharply with government data indicating that 50% of UK businesses experienced a breach or attack in the past 12 months. The discrepancy raises an important question: are respondents reluctant to disclose incidents?

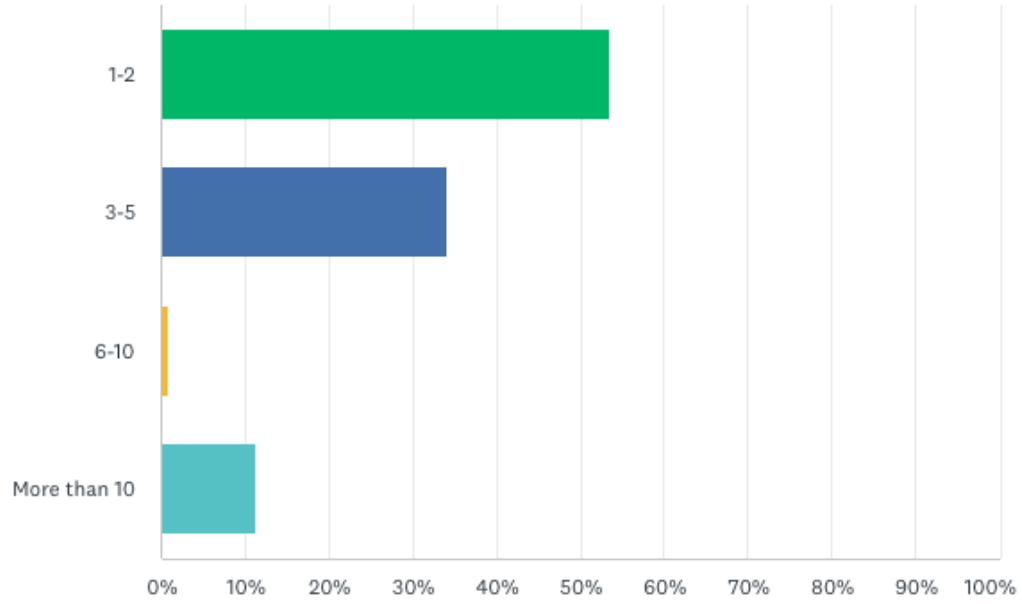
Several factors may explain this gap:

- Reputational concerns: Admitting to a breach can be perceived as a sign of weakness or poor security, even in an anonymous survey.
- Internal culture: Employees may feel pressure to present their organisation in a positive light.
- Awareness gaps: Some respondents may not know if their organisation was attacked, especially if incidents were contained without broad communication.

The 10% who declined to answer reinforces the likelihood of underreporting. Cybersecurity remains a sensitive topic, and transparency is often limited—even in research contexts.

When asked about other companies, the responses are more in line with the government figures, as shown in the next question.

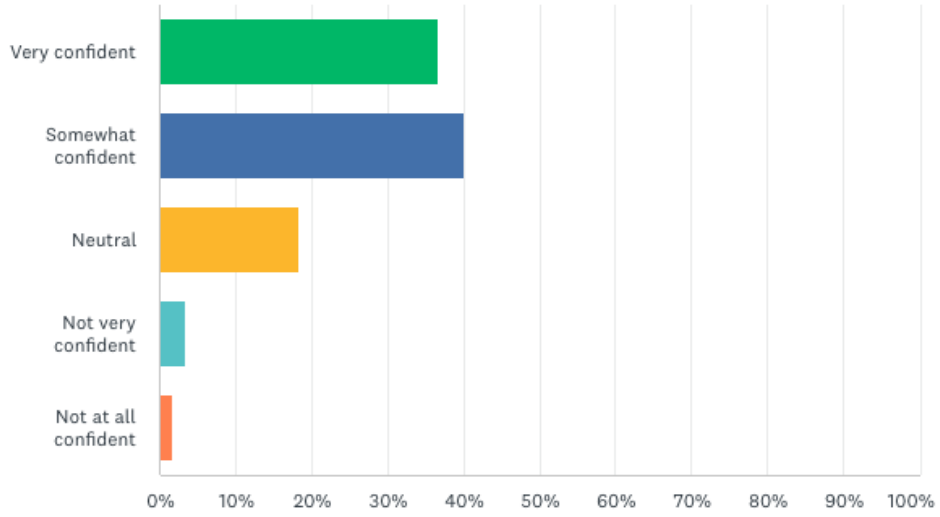
Q. 2 How many other companies in your network have experienced a cyber-attack?



- 54% said 1-2 companies had experienced a cyber-attack
- 34% said 3-5 companies had experienced a cyber-attack
- 1% said 6-10 companies had experienced a cyber-attack
- 11% said more than 10 companies had experienced a cyber-attack

As noted in our comments on the previous question, here, we see a much more expected result, with the majority of respondents being aware of one or more companies in their network having received a cyber-attack.

Q. 3 How confident are you in your organisation's ability to prevent cyber-attacks?



- 37% said they were very confident
- 40% said they were confident
- 18% were neutral
- 3% were not very confident
- 2% were not all confident

The data suggests a strong sense of assurance among respondents, with 77% expressing confidence or high confidence in their organisation's ability to prevent cyber-attacks. At face value, this is encouraging and may reflect investment in security measures, training, and governance frameworks.

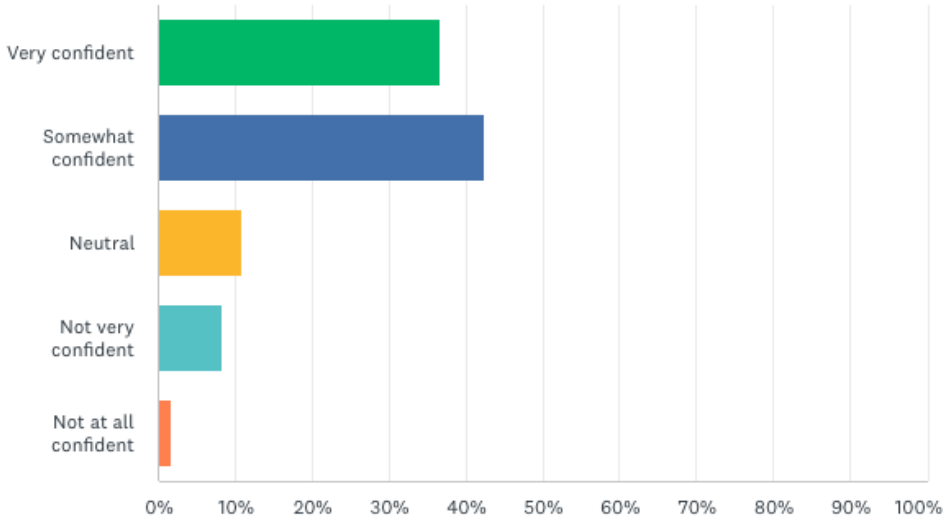
However, this level of confidence warrants scrutiny. Industry statistics and government reports consistently show that cyber-attacks remain widespread and increasingly sophisticated, affecting organisations of all sises. This raises the question: is this confidence justified, or does it indicate overconfidence and a reluctance to acknowledge vulnerabilities?

Several factors could explain this optimism:

- Internal bias: Respondents may perceive their own organisation as better prepared than others, even without objective benchmarking.
- Limited visibility: Employees may not be fully aware of gaps in systems or processes, especially if communication around risk is minimal.
- Cultural factors: Organisations often prefer to project strength in security, which can influence individual perceptions.

The risk of overconfidence is significant. If organisations underestimate their exposure, they may fail to allocate sufficient resources for continuous improvement, leaving them vulnerable to emerging threats.

Q. 4 How confident are you in your organisation's ability to recover from a cyber-attack?



- 37% said they were very confident
- 43% said they were confident
- 11% were neutral
- 8% were not very confident
- 2% were not all confident

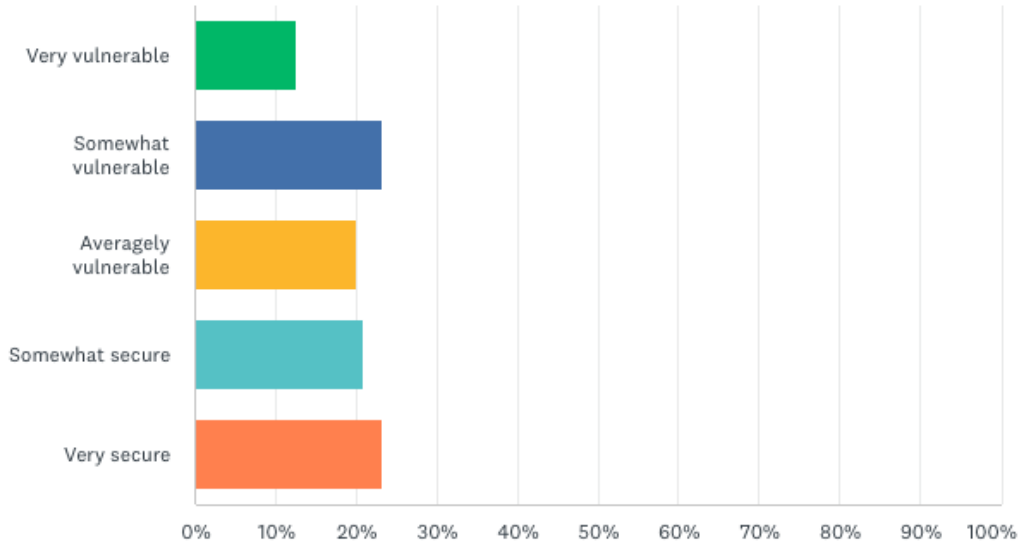
The results show that 80% of respondents are confident or very confident in their organisation's ability to recover from a cyber-attack, which is reassuring on the surface. This suggests that many organisations believe they have robust incident response plans, backup systems, and recovery processes in place.

However, this confidence should be examined critically. Recovery from a cyber-attack is complex and often involves more than restoring systems - it includes managing reputational damage, regulatory compliance, and potential financial losses. Overconfidence can lead to complacency, especially if recovery plans are not regularly tested or updated to reflect evolving threats.

The 11% neutral and 10% expressing low confidence indicate that some organisations may lack clear recovery strategies or have concerns about their resilience under real-world conditions. This aligns with findings from Q.23, where a significant proportion of organisations either do not have a regularly tested incident response plan or are unaware if one exists.

In retrospect, perhaps respondents do not wish to (be seen to) criticise their own employer, we should have asked if they had the same confidence in other companies' ability to recover. This is partly tested in the following question…

Q. 5 How vulnerable is your supply chain to cyber-attacks?

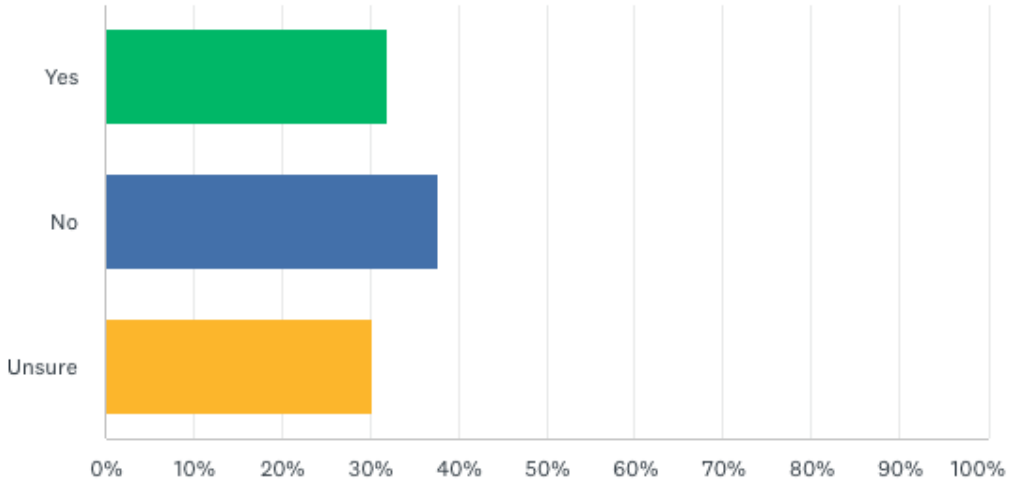


- 13% said very vulnerable
- 23% said somewhat vulnerable
- 20% said averagely vulnerable
- 21% said somewhat secure
- 23% said very secure

While respondents expressed strong confidence in their own organisation's ability to prevent and recover from cyber-attacks (Qs. 3 and 4), this confidence does not fully extend to their supply chains. Over one-third (36%) believe their supply chain is either somewhat or very vulnerable, compared to only 5% who expressed low confidence in their own organisation's resilience. This disparity suggests that organisations recognise the inherent risk posed by third-party relationships—a well-documented attack vector in recent years. Or perhaps it is overconfidence?

Supply chain vulnerabilities can arise from weaker security practices among vendors, lack of visibility into their controls, and insufficient contractual requirements. These risks are amplified by the interconnected nature of modern business ecosystems, where a breach in one partner can cascade across multiple organisations.

Q. 6 Do you believe your customers are taking sufficient cyber security measures?



- 32% said Yes
- 38% said No
- 30% said Unsure

The pattern continues when respondents assess their customers' cybersecurity posture. Only 32% believe customers are doing enough, while 38% disagree and 30% are unsure. Combined with Q.5, this indicates a broader lack of confidence in external entities—whether suppliers or clients—compared to internal capabilities. This perception gap may reflect limited transparency, inconsistent standards, or assumptions based on high-profile breaches in the market. It may also reflect an overconfidence in respondents in their own organisations capabilities.

Q. 7 Do you believe the private sector is doing enough to prevent cyber-attacks?

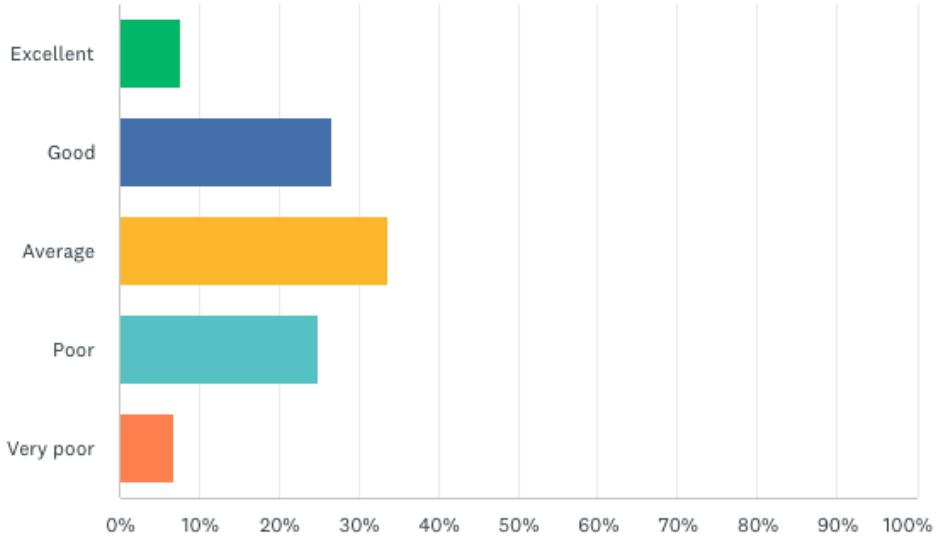
- 35% said Yes
- 46% said No
- 19% said Unsure

Q. 8 Do you believe the public sector is doing enough to prevent cyber-attacks?

- 23% said Yes
- 57% said No
- 20% said Unsure

The gap between the private sector and the public sector is considerable. Bearing in mind that most of our respondents were from the private sector, it's possible that this may reflect a feeling that is not based on direct knowledge. We don't know how many of the public sector respondents actually voted No to Q. 12, but we believe the results here reflect what we at Be-IT hear out in the market: generally, the public sector is regarded as more vulnerable than the private sector. Whether that perception matches reality would require further research.

Q. 9 How would you rate the overall vulnerability of UK organisations/companies to cyber-crime?



- 8% said Excellent
- 27% said Good
- 34% said Average
- 25% said Poor
- 7% said Very Poor

This broad view of respondents' perception of UK cyber-security—where only 35% rate it as Excellent or Good—stands in stark contrast to their confidence in their own organisation's capabilities. In Q.3, 77% expressed confidence or high confidence in their ability to prevent attacks, highlighting a significant gap between perceived national resilience and internal assurance.

Q. 10 Does your organisation have a formal cyber security policy?

- 84% said Yes
- 12% said No
- 4% said they didn't know

Q. 11 Does your organisation conduct regular penetration tests or vulnerability assessments?

- 72% said Yes
- 13% said No
- 14% said they didn't know

Q. 12 How often is cyber security training provided to employees?

- 20% said Monthly
- 30% said Quarterly
- 30% said Annually
- 9% said less than once a year
- 6% said Never
- 5% offered various other responses (e.g. 'occasional phishing test')

Q. 13 Is your organisation investing enough in cyber security?

- 51% said Yes
- 23% said No
- 26% said they didn't know

These questions are directed at the respondent's own company/organisation. Again, they elicit strong, positive responses, indicating a high degree of awareness, training and activity generally. However, once more what people think about their own company is not necessarily what they think about others. For example, here, in Q. 13, half said their organisation is investing enough in cyber security, whereas in Qs 7 and 8, when we asked respondents to think about the country more generally, the responses suggest that only 35% of the private sector and 23% of the public sector are doing enough.

Q. 14 Do we have enough skilled cyber security professionals in Scotland/UK?

- 26% said Yes
- 42% said No
- 32% said they didn't know

Q. 15 Are there enough people being trained to meet future cyber security needs in Scotland/UK?

- 40% said Yes
- 60% said No

Given that hardly a day seems to go by without another story of a major company suffering a massive cyber-attack, the answers to these two questions are concerning.

The data highlights a significant skills shortage in the cybersecurity workforce. Fewer than one in three respondents believe there are enough skilled professionals available, while 42% explicitly state there are not. The 32% who are unsure suggest a lack of visibility into the talent pipeline, which may indicate weak workforce planning or limited awareness of industry capacity. This shortage is particularly concerning given the increasing frequency and sophistication of cyber threats.

The outlook for future talent is even more worrying. A clear majority (60%) believe that current training efforts are insufficient to meet future demand. This suggests that the skills gap is not only a present challenge but a growing one, with long-term implications for organisational resilience and national security. Without significant investment in education, training, and career pathways, Scotland and the wider UK risk falling behind in the global cybersecurity race.

Q. 16 What are the biggest internal challenges to improving cyber security? Select all that apply.

- 66% said Budget constraints
- 61% said the Skills Gap
- 47% said Lack of Executive buy-in
- 45% said Low Employee Awareness

The findings reveal that financial limitations and workforce capability are the two most pressing internal challenges. Budget constraints (66%) top the list, which is unsurprising given the broader economic pressures businesses face—from rising energy costs and employer NIC contributions to new employment legislation. These factors may make it difficult for organisations to allocate sufficient resources to cybersecurity initiatives.

Close behind is the skills gap (61%), echoing earlier survey responses that highlighted a shortage of qualified cybersecurity professionals and insufficient training for future needs. This gap not only affects day-to-day operations but also limits the ability to implement advanced security measures.

The third and fourth challenges—lack of executive buy-in (47%) and low employee awareness (45%)—point to cultural and organisational issues. Without strong leadership commitment and widespread staff engagement, even well-funded cybersecurity programs can fail. Executive involvement is critical for prioritising security at a strategic level, while employee awareness is essential for reducing human error, which remains a leading cause of breaches.

Q. 17 What specific skill sets are most lacking in the fight against cyber-crime?

This was an open-ended question, with a box for comments. The Word Cloud here shows the most commonly cited words/phrases.

Q. 18 Do you believe AI is being used effectively in combating cyber-crime?

- 26% said Yes
- 37% said No
- 36% said they didn't know

The responses to this question reveal an important indicator of current perceptions and maturity levels regarding the use of artificial intelligence in cybersecurity operations. Only 26 percent of respondents believe that AI is being used effectively to combat cyber-crime. By contrast, a slightly higher proportion (37 percent) do not see it as effective, and a further 36 percent admit they don't know.

This distribution shows that confidence in AI's cyber defense capabilities remains lukewarm across the sample. The near-equal split between "No" and "Don't know" suggests uncertainty and perhaps limited visibility into how AI is currently deployed in real-world threat detection, intelligence, and mitigation functions. Many organisations may still view AI in cybersecurity as more of a conceptual promise rather than a widely adopted and proven technology.

The high "Don't know" response group is particularly telling. It reinforces that, for many, AI remains something talked about in industry reports and vendor marketing rather than a transparent, operationally integrated component of their security infrastructure. This perception gap may stem from several factors:

- Limited communication from cybersecurity teams about the role AI tools play in daily defensive operations.

- A lack of measurable success stories on AI-led threat prevention and incident response.
- Early-stage adoption, where benefits are still emerging or difficult to quantify.

The data likely reflect where the industry currently stands on the adoption curve—AI has significant potential but is not yet fully trusted nor clearly understood outside specialist circles.

Q. 19 Does it matter if cyber security providers are based overseas?

- 40% said Yes
- 46% said No
- 13% said they were Unsure

The responses reveal a divided perspective among IT professionals. While a slight majority (46%) believe provider location does not matter—likely influenced by the widespread adoption of remote work and cloud-based security solutions—the 40% who answered "Yes" indicate a significant concern about geographic proximity. This concern is understandable given the current global security climate, where geopolitical tensions and cross-border cybercrime are increasingly prevalent. For these respondents, domestic providers may represent greater trust, regulatory alignment, and perceived control over sensitive data.

The 13% who were unsure suggest a knowledge gap regarding the implications of provider location, such as compliance with data sovereignty laws, risk exposure, and contractual enforcement across jurisdictions. This uncertainty presents an opportunity for organisations to educate stakeholders on how overseas partnerships are managed securely.

Q. 20 What will be the most important issues in the future for fighting cyber-crime?

This was an open-ended question, with a box for comments. The Word Cloud here shows the most commonly cited words/phrases. The fact that AI stands out so clearly supports our argument in Q. 18 above.


infrastructure
AI-powered threat
education
threats
new
issues
include
security
AI
attacks
cyber
Awareness
Trained
will
data
secure
needed
cloud
future
quantum computing

Q. 21 Does your organisation have a dedicated Chief Information Security Officer (CISO) or equivalent role?

- 55% said Yes
- 29% said No
- 5% said Planning to Hire
- 10% didn't know

Q. 22 How involved is your executive leadership in cyber security strategy?

- 39% said Very Involved
- 44% said Somewhat Involved
- 11% said Rarely Involved
- 10% said Not Involved at all

These questions give us an idea of how seriously cyber-security is taken at a senior level in companies. It is gratifying to see that a majority of our respondents' organisations have a CISO and that the vast majority (83%) say their executive team is either very or somewhat involved in strategy. However, as the responses elsewhere suggest, to say nothing of the government figures cited in the introduction, there is an imperative need for ALL senior management to be not just aware of but also cognisant with the modern requirements of cyber-security and thus competent to create (alongside their IT professionals) strategies to minimise risk. This is, to some extent, borne out by the response to the next question, where only half have a regularly tested incident response plan in place.

Q. 23 Do you have a cyber incident response plan in place?

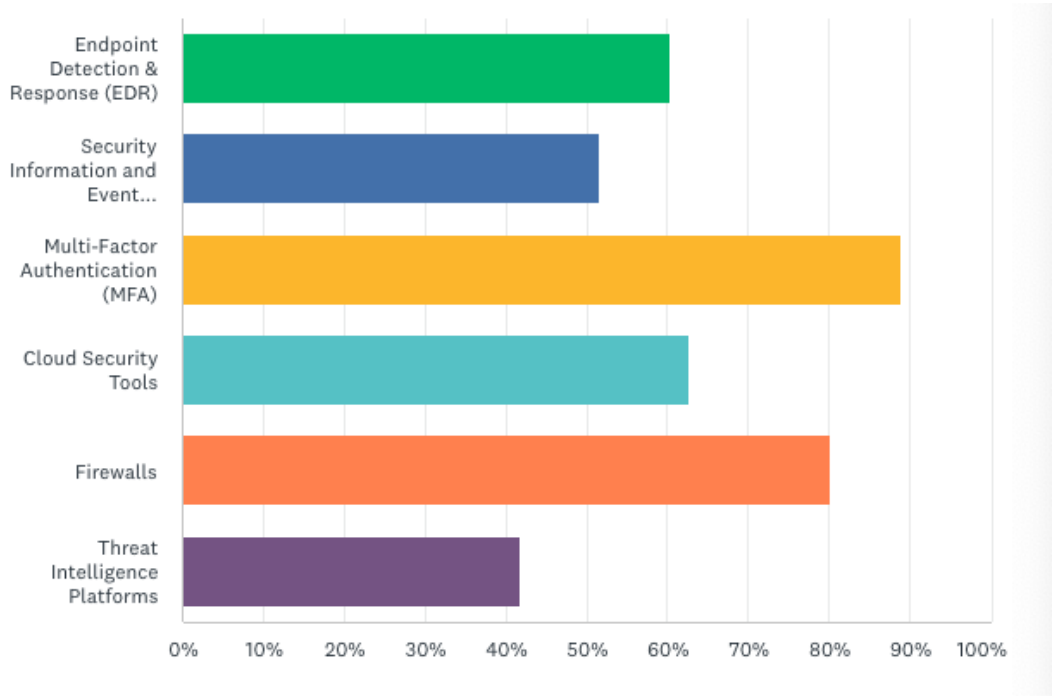
- 50% said Yes, and it is regularly tested
- 27% said Yes, but it is not regularly tested
- 10% said No
- 13% didn't know

The results show that while half of respondents have a regularly tested incident response plan—a positive indicator of maturity—there is still a significant gap in preparedness. The 27% who have a plan but do not test it regularly represent a critical vulnerability; an untested plan may fail under real-world conditions, leading to delayed response and increased impact during an actual incident.

The 10% without any plan and the 13% who are unaware of whether one exists highlight a concerning lack of visibility and governance. In today's threat landscape, where cyberattacks are increasingly sophisticated and fast-moving, the absence of a tested response plan can result in severe operational, financial, and reputational damage.

These findings suggest that while progress has been made, organisations must prioritise regular testing, staff awareness, and clear communication of incident response protocols. Testing ensures that roles, responsibilities, and technical processes are effective under pressure, while awareness reduces confusion during a crisis.

Q. 24 Which of the following technologies does your organisation currently use for cyber security? (more than one could be ticked)



In order, the most popular are:

- Multi-factor authentication: 89%
- Firewalls: 80%
- Cloud security tools: 63%
- Endpoint Detection & Response: 60%
- Security Information & Event Management: 52%
- Threat intelligence platforms: 42%

Q. 25 Do you assess the cyber security posture of third-party vendors or partners?

- 31% said Yes, regularly
- 38% said Occasionally
- 12% said No
- 19% were Unsure

These results indicate a significant gap in third-party risk management. While 31% of respondents regularly assess vendor cybersecurity posture—a positive sign—nearly half (38%) only do so occasionally, and 12% do not conduct assessments at all. The 19% who are unsure suggest a lack of visibility or unclear responsibility for vendor risk within their organisations.

This is concerning because third-party relationships are a well-documented attack vector. Weak security practices among vendors can create indirect vulnerabilities. When vendors are compromised, attackers can exploit trusted connections to gain access to internal systems, effectively creating back doors into the organisation. High-profile breaches in recent years have demonstrated how devastating these indirect attacks can be.

The findings highlight the need for consistent, structured vendor risk assessments as part of a broader cybersecurity strategy. Occasional checks may not be sufficient given the dynamic nature of threats and the increasing reliance on external partners for critical services.

Q. 26 Is your organisation required to comply with any cyber security regulations or standards (e.g. ISO 27001, NIST, GDPR)

- 70% said Yes
- 15% said No
- 15% said they don't know

The results show that compliance with cybersecurity regulations and standards is a major factor for most organisations, with 70% confirming they are subject to such requirements. This is unsurprising given the growing emphasis on data protection, privacy laws, and industry-specific mandates. Compliance frameworks like ISO 27001, NIST, and GDPR not only help organisations meet legal obligations but also serve as benchmarks for best practice in risk management.

However, the 15% who do not comply and the 15% who are unsure raise concerns. Lack of awareness or clarity around compliance obligations can expose organisations to regulatory penalties, reputational damage, and increased vulnerability to cyber threats. The "don't know" responses suggest gaps in governance and communication, particularly in ensuring that IT teams understand the regulatory landscape affecting their operations.

As regulatory requirements continue to evolve globally, organisations must prioritise compliance awareness, clear accountability, and regular audits to maintain trust and resilience.

Q. 27 Would your organisation consider outsourcing cyber security services to a third-party provider?

- 26% said Yes
- 35% said No
- 10% said they already do
- 29% said they were Unsure

There is a mixed response here, with over one third saying they would not outsource their cyber security to a third-party, but the same percentage (35%) saying either that they already do (10%) or that they would (25%). Almost 30% said they were unsure. Overall, this suggests there may well be a substantial market for reputable, reliable third-party providers of cyber security. Following on from this, our next question asked what types of external support companies would find most useful…

Q. 28 What types of external support would be most valuable to your organisation? (Select all those that apply)

- Staff training and awareness: 67%
- Compliance and audit support: 57%
- Cyber security consulting: 54%
- Managed detection and response (MDR): 47%
- Incident response services: 42%
- Recruitment of cyber security talent: 32%

The responses highlight that human factors and regulatory compliance remain top priorities for organisations. The fact that 67% identified staff training and awareness as the most valuable support underscores the persistent challenge of human error in cybersecurity incidents. This aligns with industry data showing that phishing and social engineering attacks often exploit gaps in user awareness. This also aligns with the gaps in knowledge that answers to previous questions have identified.

Compliance and audit support (57%) and consulting services (54%) also rank highly, reflecting the complexity of navigating evolving regulatory requirements and the need for expert guidance in building robust security strategies.

Meanwhile, nearly half of respondents (47%) see value in managed detection and response (MDR), indicating growing recognition of the importance of proactive threat monitoring and rapid response capabilities.

Interestingly, incident response services (42%) and cybersecurity talent recruitment (32%) are lower priorities, which may suggest that organisations either feel reasonably confident in their internal capabilities or underestimate the difficulty of sourcing skilled professionals—a known industry challenge.

Overall, these findings suggest that organisations are seeking a balanced mix of education, compliance support, and technical expertise, with a strong emphasis on preventative measures through training and awareness.

APPENDIX

Q. 1 Job titles (duplications, of which there were a lot, have been removed)

Responses
Applications Consultant
Automation test engineer
Business analyst
Business Development Manager
CEO
Chief architect
Client Director
Cloud & Infrastructure Manager
Cloud Engineer
Cloud support Engineer
Code Facilitator
Compliance OfficerConsultant
Consultant Project/Programme Manager
Crime Analyst
CTO
Cutover Manager
Cyber and Cloud Security Expert
Cyber Culture Lead
Cyber Recruiter
Cyber Risk
Cyber risk and assurance manager
Cyber Security Engineer
Cyber Security Manager
Data analyst
Data engineer
Data Manager
Design Lead
Developer
Developer / Director
Development team lead
DevOps
DevOps engineer
Digital forensic
Digital Trainer

Director
Dotnet Developer
Economic Crime Risk Officer
Endpoint Engineer II
Engineering Manager
Financial project manager
Frontend Engineer
Head of AFC
Head of IT
Head of Product
Head of Risk and Information Security
Head of Technology
Healthcare Assistant
Implementation Manager
Information Security Risk & Assurance Manager
Infrastructure architecture
Infrastructure Specialist
IT & Technical Manager
IT consultant
It engineer
IT infrastructure engineer
IT Manager
IT manager
IT Project Manager
IT Security Analyst
It strategy consultant
IT support engineeer
IT support Engineer
IT Systems Engineer
Learning Technology Specialist
M365 Tech Lead
Managing Director
Marketing Freelancer
Marketing mamager
Mobile Application Developer
Operator
Platform Engineer
PMO Lead
Product Manager
Programme Manager
Project Coordinator (IT)

Project management
Project manager
Python Engineer
QA
QA Engineer
qa engineer
Readiness lead
Researcher
Retail
Sales Consultant
Senior AI Engineer
Senior Anaplan Analyst
Senior Business Analyst
Senior Change Manager
Senior CSM
Senior Engineering Manager
Senior InfoSec Consultant
Senior IT Consultant
Senior Software Engineer
Senior Test Analyst
senior test analyst
Service delivery manager
Service Delivery Project Manager
Software Engineer
Software Engineer Team Lead
software tester
Solution Designer
Staff QA Engineer
Support Analyst
Talent Acquisition Consultant
Technical Planning Manager
Technology Director
Test Consultant
Test lead / Manager
Tutor
UX Designer