Bytes Cyber Security

Market Report | Autumn 2024

In Proud Partnership with
CATO Networks

Introduction

First and foremost, I want to express my gratitude to everyone who participated in our survey. The insights we gathered are not only fascinating but will also enhance our continuous efforts to serve our customers better, and add significant value to the broader industry.

So far in 2024, the cyber security landscape has been shaped by heightened geopolitical tensions, leading to more sophisticated state-sponsored attacks and therefore, it's no surprise to see the number one challenge in the survey as "increased sophistication of phishing attacks". This is compounded by the rise of generative AI, which in itself, is a double-edged sword. Generating new vulnerabilities, but also exciting opportunities for better security.

Many organisations are finding it tough to keep up with fast-evolving threats due to a significant skills shortage. However, there's been a big shift towards partners offering Managed Security Services to help tackle this issue.

Many of the breaches reported in the industry over the past year have stemmed from third-party or supply chain vulnerabilities. This issue has climbed up the priority list in our recent surveys. As we increasingly rely on third-party suppliers, it's clear that more investment will be needed to address these risks.

We've also seen refreshed/new compliance standards coming into play to keep up with the changing landscape. From these we are seeing an increasing demand in certain solution/ service areas, such as Incident Response, which took the top spot in this survey for customer priorities.

To close out, over the past year, the UK Cyber Security sector has shown impressive growth, with revenue up by 13% and 2,700 new jobs created. This really highlights the industry's impact and importance across all verticals[1].

By **Luke Kierman** | Head of Cyber Security at Bytes.

With additional commentary and insights provided by:

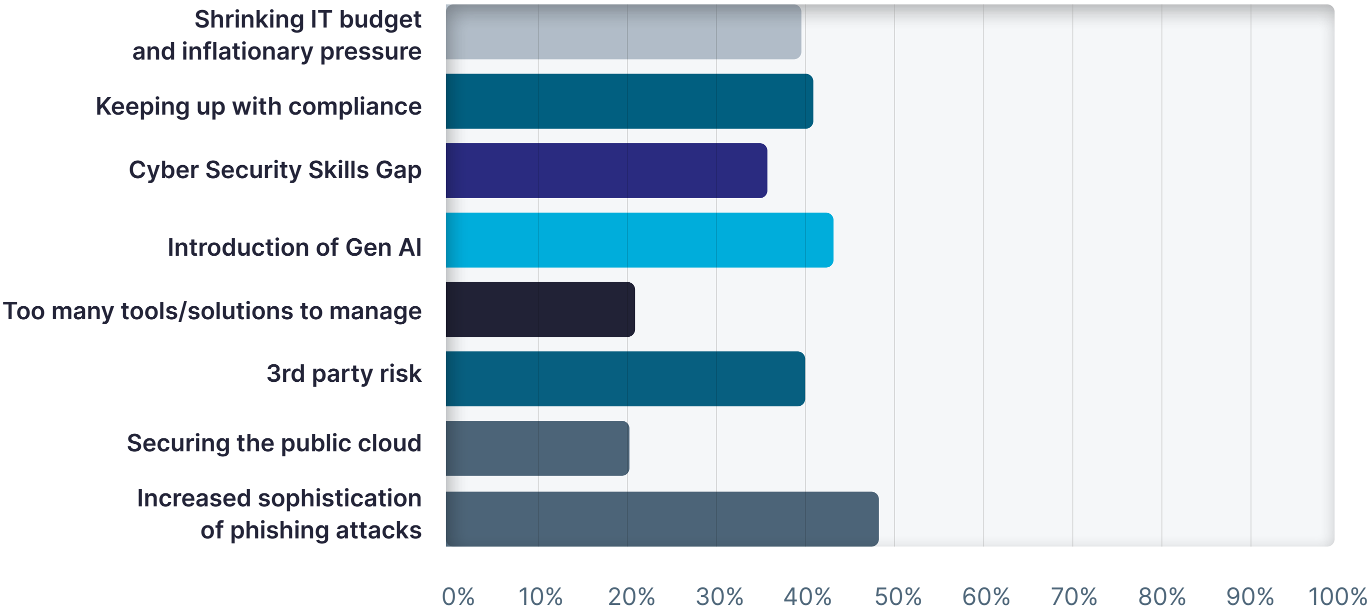
Giuseppe Damiano, Pre-Sales Solution Consultant, Bytes
Ellen Hallam, Threat Intelligence Analyst, Bytes
Urfan Iqbal, Cyber Consulting Pre-Sales Specialist, Bytes
Etay Maor, Chief Security Strategist, CATO Networks

[1] Cyber security sectoral analysis 2024 - GOV.UK (www.gov.uk)

Q1.

What do you foresee as the biggest cyber security challenge of 2024/2025?

(Select your top three)



Summary

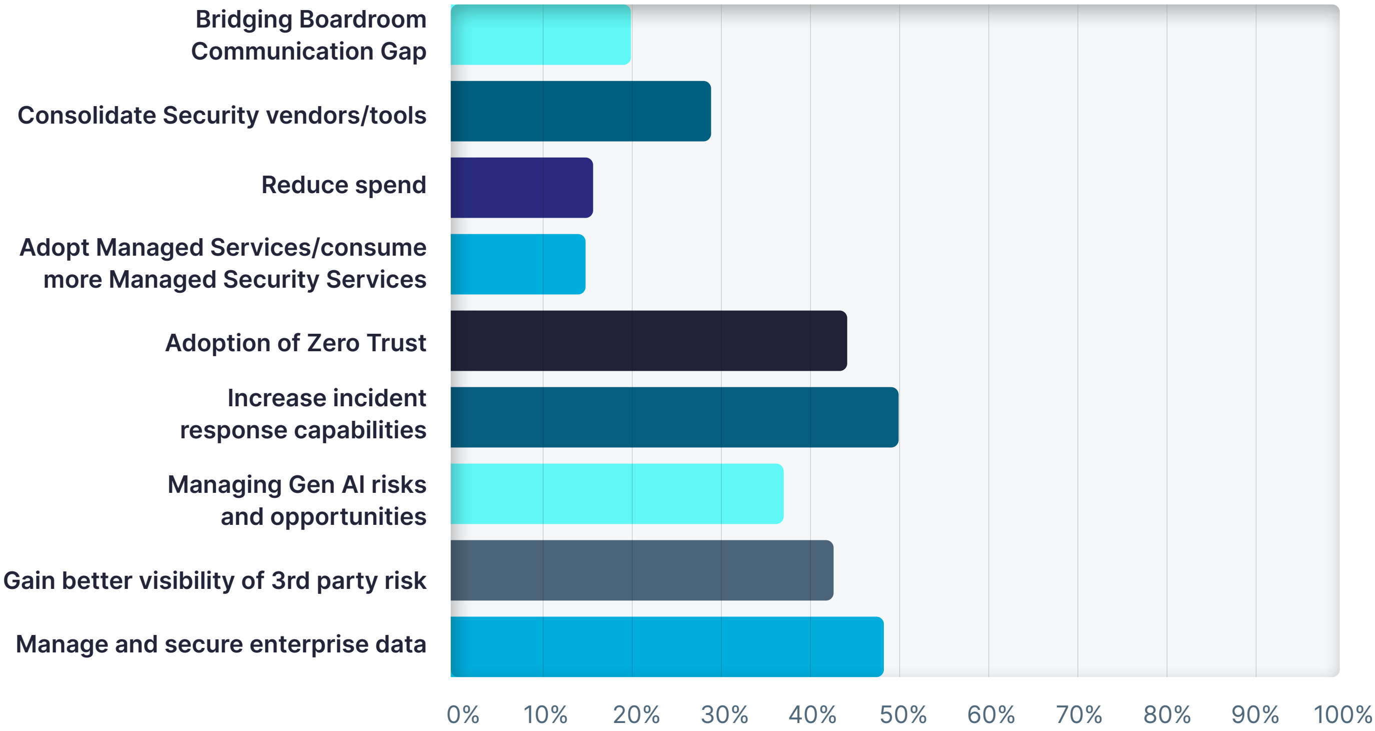
Respondents are right to be concerned by the threats posed by Gen AI as criminal organisations are successfully using it to craft ever more realistic phishing attacks – making them more effective at disarming the target and achieving their aim.

Criminal gangs are also finding it can be easier to breach third party organisations that supply goods or services to their primary targets than it is to breach their primary targets. Because of this, they are more pervasively targeting supply chains as a means of entry and leverage into their primary targets.

Q2.

What are your top three cyber security priorities for 2024/2025?

(Select three options)



Summary

For reasons given in the summary from the last question, and specifically the increasing success rate of (Gen AI-powered) sophisticated phishing attacks, it is a question of "if" and not "when" an organisation is subjected to a potentially harmful attack. It is logical therefore that "Increasing incident response capabilities" is at the top of the priority list for many organisations. The need for organisations to continually test the robustness of their incident response capability is also essential as threats, people's knowledge and managed security services are constantly evolving, so to be sure incident response processes are still effective, they need to be regularly scrutinised.

It is encouraging to see "Manage and secure enterprise data" so high up the list as the

Summary contd...

Q2. contd

What are your top three cyber security priorities for 2024/2025?

Summary contd

discovery, classification, deletion, move, security and assignment of access rights is something that does not always get the attention it deserves yet is an essential part of having a good and well-maintained security posture. If an organisation knows where their data is, particularly their sensitive data, has taken steps to protect it and has put the necessary access rights in place, the risk of threats towards data will be materially lower in the event of a security breach.

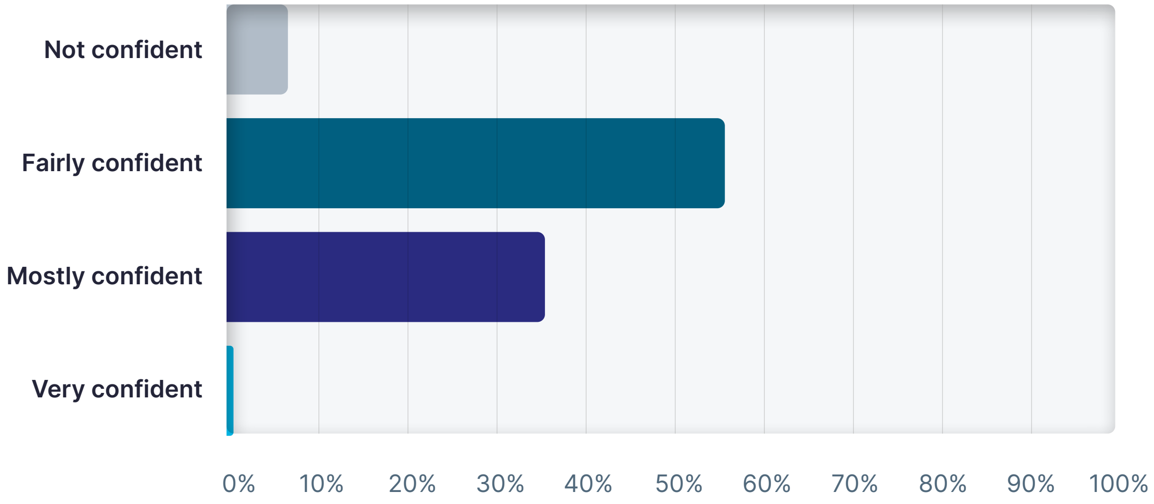
With Copilot and other GenAI models being deployed throughout Enterprises, it is also more important than ever for organisations to properly classify and protect their data to avoid data overexposure incidents, either accidental or malicious. The use case of an employee seeing information they shouldn't see (salary details, critical systems credentials, etc) as a response to a GenAI prompt query is one that resonates to all organisations who have explored these technologies.

The other priorities in this question are reasonably in line with what we see and hear from our customers, except for the consolidation of security vendors. Having a consolidation strategy can significantly improve an organisation's ability to respond to threats due to simplified training for members of IT staff. Consolidation can also contribute to an improvement in threat detection and response activities thanks to the unified nature of the security controls employed.

By their very design, the security posture of ““Frankenstein” solutions” that consist of several tools from different vendors are always going to feature a high operational and training overhead as well as a higher overall cost in procuring, managing and maintaining them.

Q3.

How confident are you about the security controls in place for 3rd party/supplier access into your network?



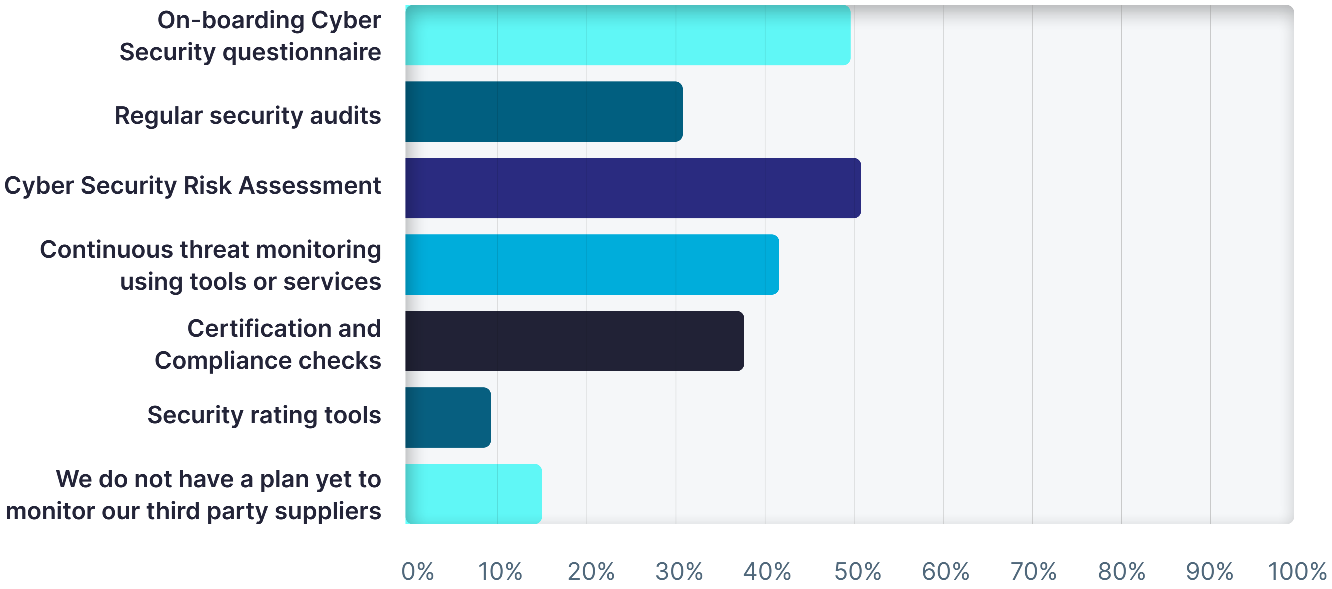
Summary

While a critical element of an organisation's overall security strategy, managing the security measures of third parties is not trivial, especially when they do not share the same interest and concerns around cyber security and associated risks due to their partnership not being related to cyber security. Supply-chain management is a necessary process that requires a balance of interests and commitments in terms of security and governance, especially in relation to customer-data, as failure to build a robust process could result in serious consequences as shown on many occasions by national news.

Q4.

How does your organisation access and manage the cyber security risks associated with third party suppliers?

(Multiple choice)



Summary

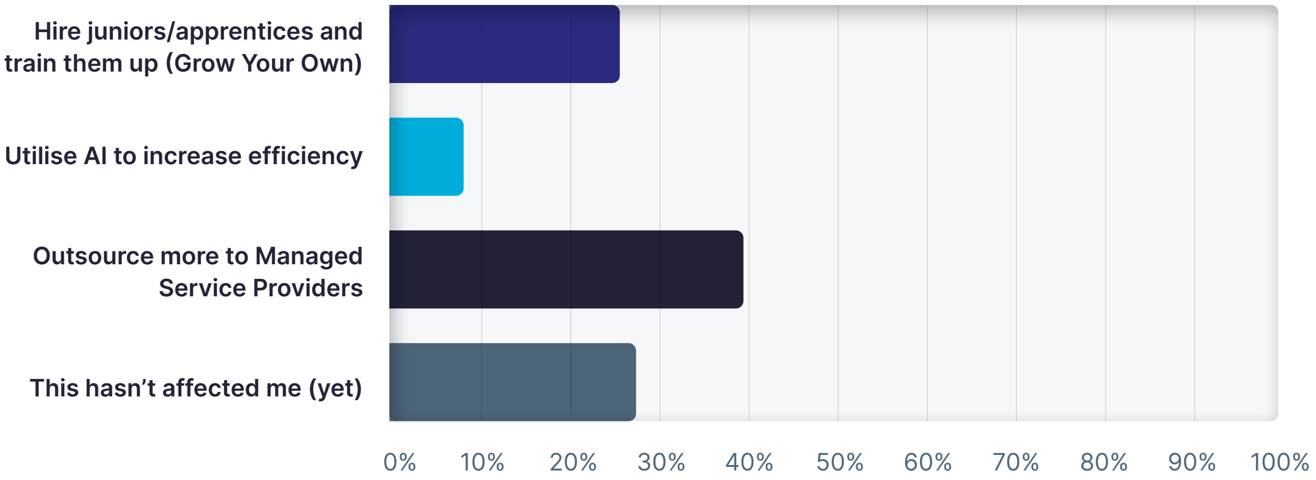
Given the balance that organisations need to strike with their suppliers and business partners, it makes sense for them to start with a cyber security risk assessment – assuming of course that the corresponding questionnaires ask the right questions and relate to universally recognised frameworks to have sufficient relevance to hold suppliers to account should the worst happen.

One way to validate suppliers is to request and scrutinise the compliance accreditations or certifications they have. It is surprising to observe that certification and compliance checks are not higher up the list with those responding to this question. In addition to point in time certifications that suppliers say they hold, it is also good practice to check how long they have held them for and to perform these checks on a regular basis.

Q5.

What is your current approach to dealing with the skills gap?

(Select one)



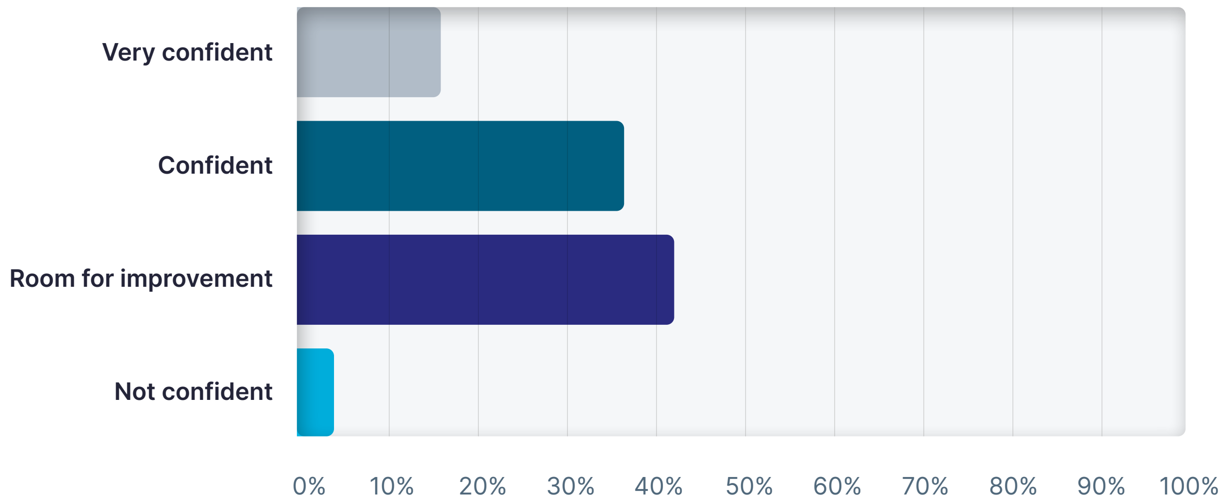
Summary

The utilisation of AI in dealing with the skills gap is going to continue to increase. AI can already write code, configure firewalls and do a lot of work that used to require highly skilled experts. With the rise and normalisation of AI in the workplace, those same skilled experts can turn their attention to other matters, such as inspecting or enhancing the work done by AI.

Q6.

How confident do you feel that your Board of Directors understand how to prioritise and invest in cyber security?

(Select one)



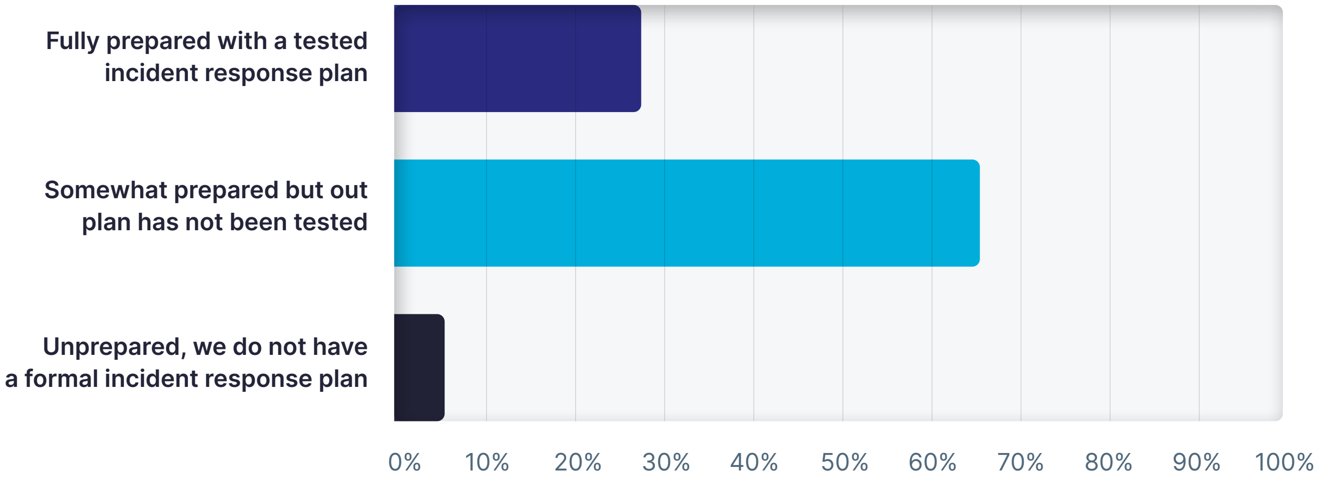
Summary

It is alarming to see that, despite the heightened tensions created by the geopolitical events affecting the world today together with the news constantly reporting successful cyber-attacks, nearly 50% of Boards are either unsure whether to prioritise cyber security, or unsure how to invest in it.

UK and global regulators all have legislation that clearly state the responsibility of company Directors around maintaining good security and data management practices. Although this is not mandatory, it is therefore good practice for security professionals to ensure they are helping to educate their Senior Leadership Team on subjects such as value and risk as it shows a level of maturity and awareness that can only support an Organisation's reputation to their customers.

Q7.

In the event of a cyber security breach, how prepared is your organisation to respond?



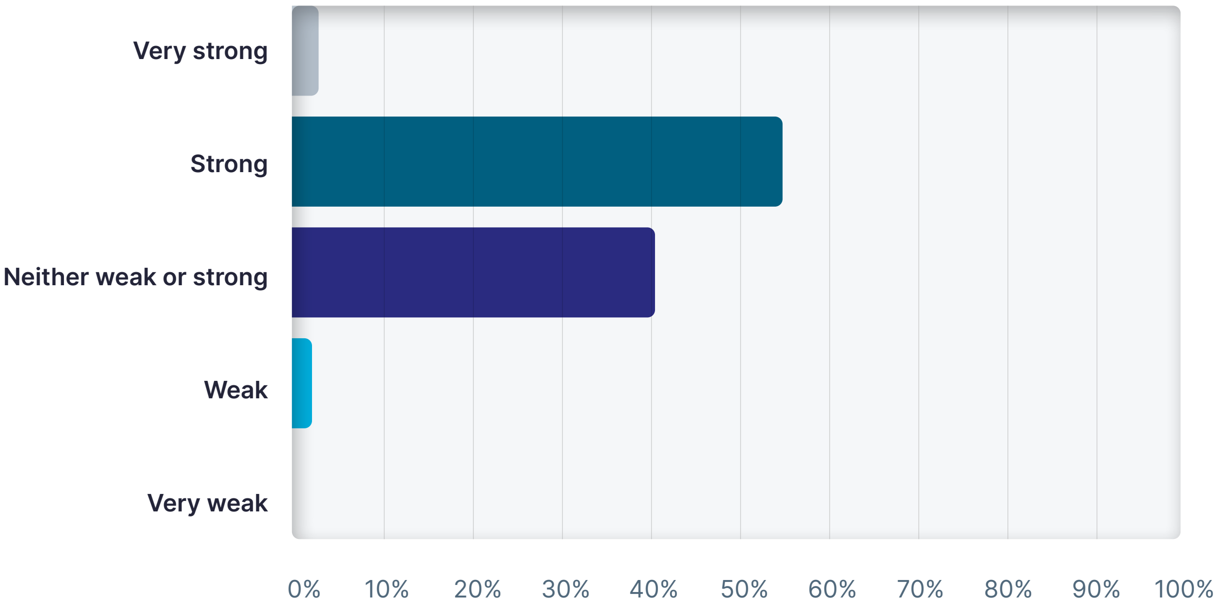
Summary

Given the findings from the last question, this is not surprising but equally worrying. More than 70% of respondents said they are only somewhat prepared or unprepared. This explains – at least in part - why most respondents to the second question cited “Increase incident response capabilities” as their main current priority. As security teams acknowledge that they are going to suffer a cyber incident, and accept they are not ready or prepared for one, they realise that something needs to be done about it as a matter of urgency.

Q8.

How well would you rate your security posture in cloud environments?

(Select one)



Summary

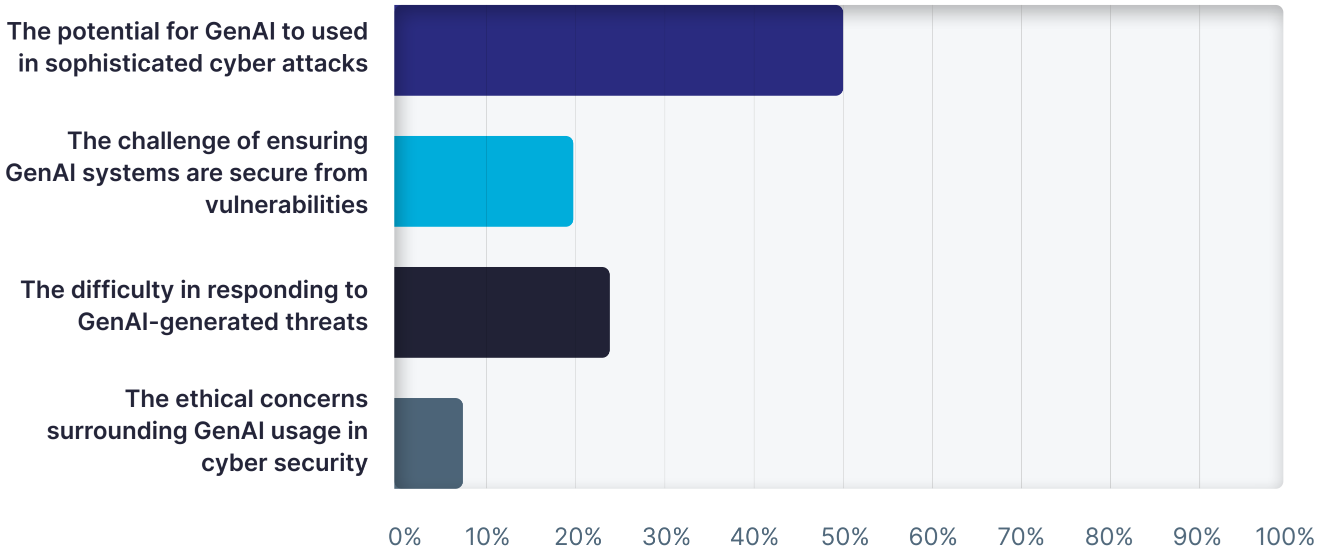
As more organisations move data to the Cloud, the Cloud is becoming more of a target for Threat Actors, meaning Defence in depth has to be considered around both Cloud and on-premise infrastructure.

Organisations that know they are exposed or think they are exposed should - as a priority - assess the extent of their cyber exposure by either conducting an internal review or commissioning a third party to do so. Appropriate resourcing can then be made to ensure any areas of high risk are addressed in an appropriate and timely manner.

Q9.

What do you perceive as the biggest cyber security risk associated with GenAI?

(Select one)



Summary

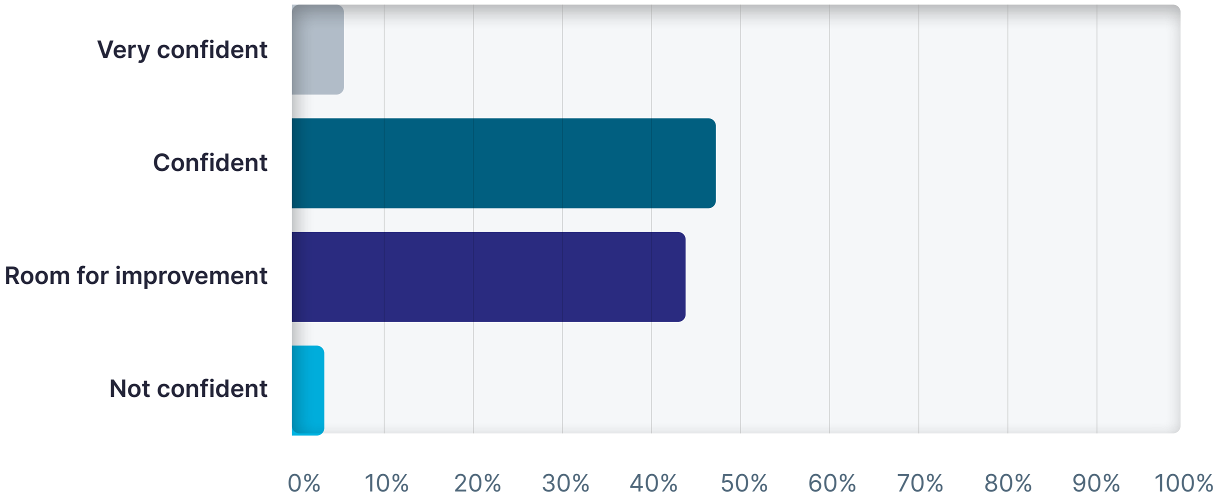
The findings from this question underscore the earlier comment that while GenAI generally poses a growing threat, the highest risk is in relation to more sophisticated phishing attacks where it is most pervasive.

GenAI today can create highly believable voice and video deepfakes that are being deployed very effectively to deceive and take advantage of targets. This technology, if left unchecked, has the potential to grow in both sophistication and scale with the consequent increase in the risk of damage for any and all organisations.

It is essential for organisations to keep up to date with new threats and to take appropriate measures to educate their employees on what to look out for. It is equally important that access rights to sensitive information are constantly reviewed and adjusted when required. This, together with a strong process around data discovery, classification and loss prevention, can significantly reduce the risk of reputational or financial damage for an organisation.

Q10.

How confident are you in your ability to detect and prevent malicious insider activity?



Summary

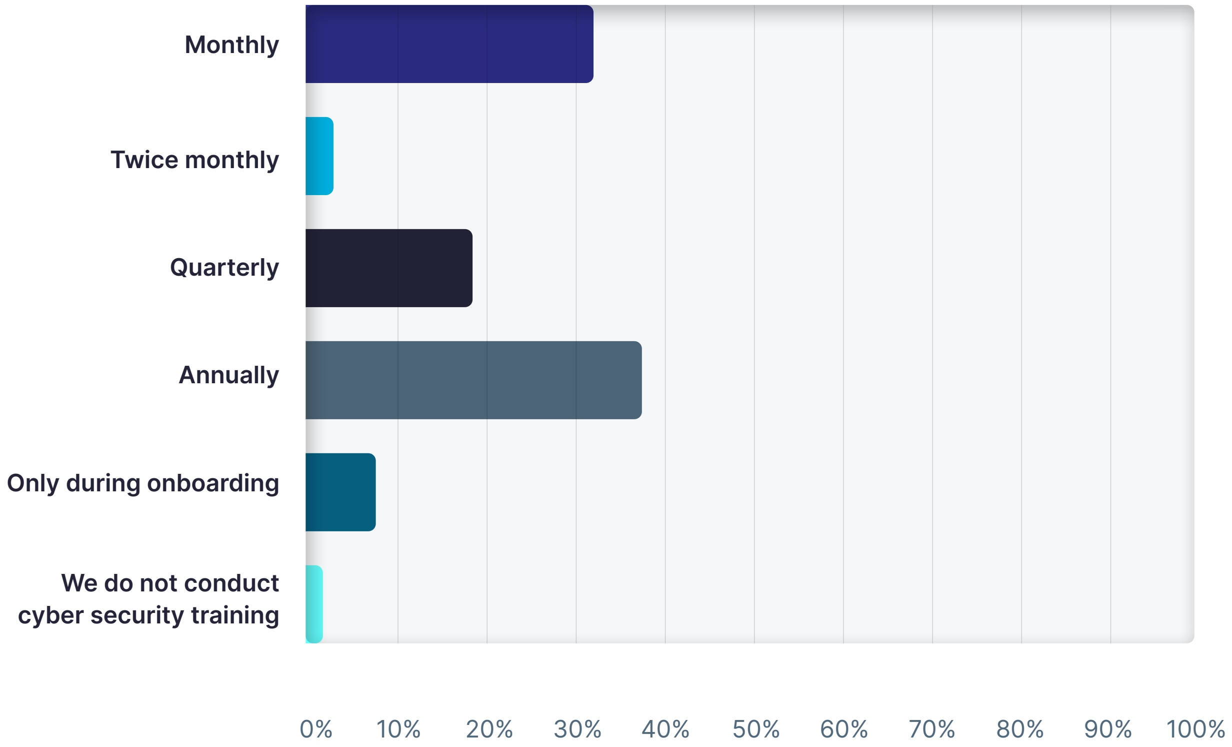
There is a common theme across previous answers in this report where organisations are generally not completely confident with their security posture. The responses from this question are not different, with over 40% of respondents saying they are either not confident or consider there to be room for improvement when it comes to detecting and preventing malicious insider activity.

There are measures organisations can take that limit access to high value data that can be stolen, copied, or encrypted unlawfully. These include privileged access management, network segmentation, and asset inventory management that prevents unrecognised assets being granted access to a company's estate.

A third-party security health check from Bytes will highlight insider vulnerabilities and document quick wins to mitigate against any associated risks.

Q11.

How often does your organisation conduct cyber security training for employees?



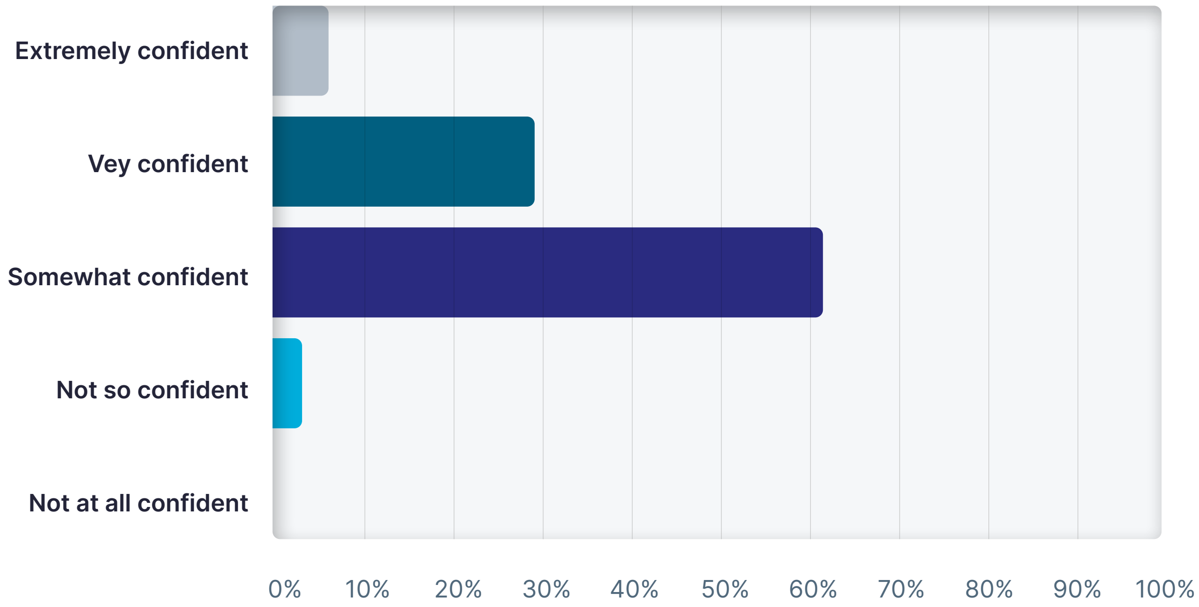
Summary

Those organisations that only conduct security training annually or once - during onboarding - open themselves up to unnecessary exposure, particularly given that most employees are not IT savvy and do not consider focussing on spotting indicators of an attack as their primary responsibility.

Regular simulated attacks, supported with general awareness communications and training, are an effective mean to minimise successful breaches by heightening the security awareness of employees.

Q12.

How confident are you that your organisation could prevent a phishing attack?



Summary

The findings from this question show once again, and rather worryingly and surprisingly, that most organisations are at best somewhat confident with their security posture. In this specific case, 65% of respondents are either not confident or somewhat confident in their organisation's ability to prevent a phishing attack.

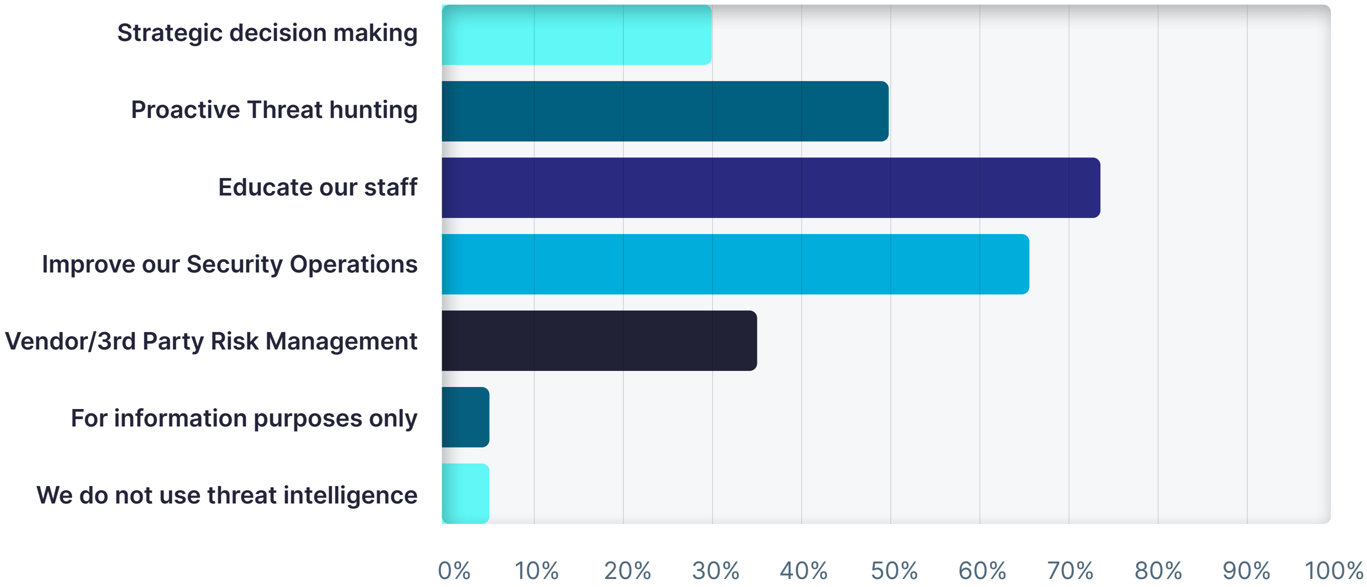
Given that only 32% of respondents from the last question conduct cyber security training monthly and that less than 30% of question 7 respondents feel they are prepared to respond to a cyber-attack, there is an alarmingly large number of organisations who appear to have either succumbed to the thought that they inevitably will suffer an attack no matter what they do, or simply do not have the will or resources to do something meaningful about it.

Whatever the reason, Bytes have a highly experienced cyber security team who can help organisations assess the efficacy of their security posture and provide a detailed roadmap of how to improve it.

Q13.

How does your organisation utilise threat intelligence to enhance its cyber security measures?

(Select those that apply)



Summary

It is encouraging to see organisations using threat intelligence to inform their decisions over how best to enhance their cyber security measures.

The 9% of respondents who either do not use threat intelligence or use it for information purposes only might be opening themselves up to an avoidable cyber attack.

Bytes Cyber Security Market Report
Autumn 2024

About Bytes Cyber Security

Bytes' Cyber Security Division is a leading provider of comprehensive IT security solutions with over 25 years of experience. They focus on delivering end-to-end and integrated cyber security services, including consultancy, solutions, and managed services. Their approach is consultancy-led, ensuring they understand clients' challenges and business goals to provide innovative and relevant security solutions.

About Cato Networks

Cato Networks is a prominent company in the field of Secure Access Service Edge (SASE) technology. Founded in 2015, Cato Networks offers a cloud-based platform that integrates enterprise communication and security services. Their platform combines SD-WAN (Software-Defined Wide Area Network) with a comprehensive suite of security features, such as threat prevention, data protection, and incident detection and response. This integration allows businesses to replace traditional, costly infrastructure with a more flexible and scalable solution. Cato Networks has been recognized for its innovative approach and has been named a leader in the Gartner Magic Quadrant for Single-Vendor SASE.

A Powerful Partnership

Bytes and Cato Networks have a strong and strategic partnership. Bytes is a leading reseller of Cato Networks' solutions, offering extensive technical expertise around Cato's Secure SD-WAN, next-generation firewall, and Cato Cloud solutions. This partnership allows Bytes to provide their customers with a cloud-based, secure global SD-WAN, which simplifies and secures their network infrastructure. Recently, Bytes was named the Cato Networks EMEA Reseller Partner of the Year for 2024. This recognition highlights the strength and growth of their partnership, as well as their joint commitment to delivering world-class security solutions to customers. The collaboration between Bytes and Cato Networks includes multiple joint go-to-market initiatives, customer events, and campaigns.

UK Head Office
Bytes House
Randalls Way
Leatherhead
Surrey
KT22 7TW

01372 418 500
tellmemore@bytes.co.uk
bytes.co.uk