BYTES | Smarter together

Cyber Security Report 2023

A Bytes Market Report

Introduction

2022 was a year of political and economic turbulence, and with it has come a further evolution of the security threat landscape.

With so much uncertainty to deal with, organisations have had to work harder than ever to ensure they keep their data and IP safe, while managing fluctuating costs, and an increasingly demanding hybrid workforce.

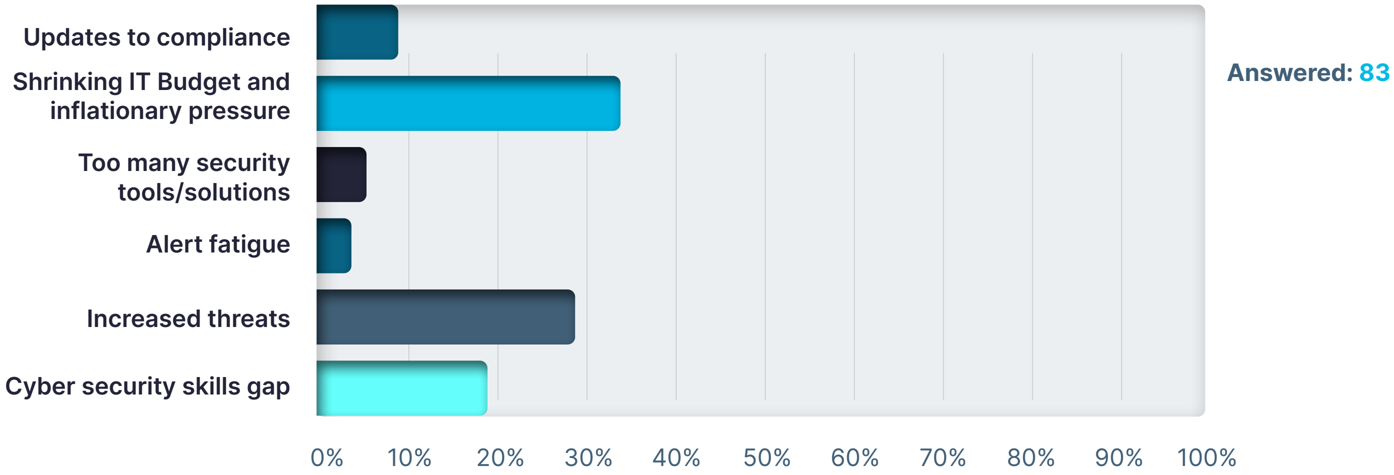
To better understand key security priorities and forecast trends for 2023, Bytes surveyed 84 IT and Security Professionals across all verticals.

This Bytes Market Report provides valuable insight into the findings, including expert reviews and commentary from Gennaro Migliaccio (Head of Solution Development at Bytes), Adam McCaig (Cyber Security Evangelist at Bytes), and Luke Kiernan (Head of Cyber Security at Bytes).

If you would like discuss the findings of this Bytes Market Report with a specialist, or are keen to understand how Bytes can optimise your 2023 Cyber Strategy, reach out to your dedicated Account Manager, or email tellmemore@bytes.co.uk

Q1.

What do you foresee as the biggest challenge of 2023? Please select one option



Summary

Although shrinking budgets is highlighted as the biggest challenge, this is not what we are seeing in the field. Budgets have certainly been impacted by the recent exchange rate fluctuations, inflation figures, and news of a recession but we are seeing more of a pause rather than a reduction in spend.

The weighting of the "Increased Threats" option is interesting as this is certainly a matter of perception. The level of threats has been reasonably continuous throughout 2022 and it is interesting to observe that our customers are feeling and/or observing higher levels of risk in 2023. The risk landscape will undoubtedly evolve throughout 2023, so it is crucial that all organisations remain on high alert.

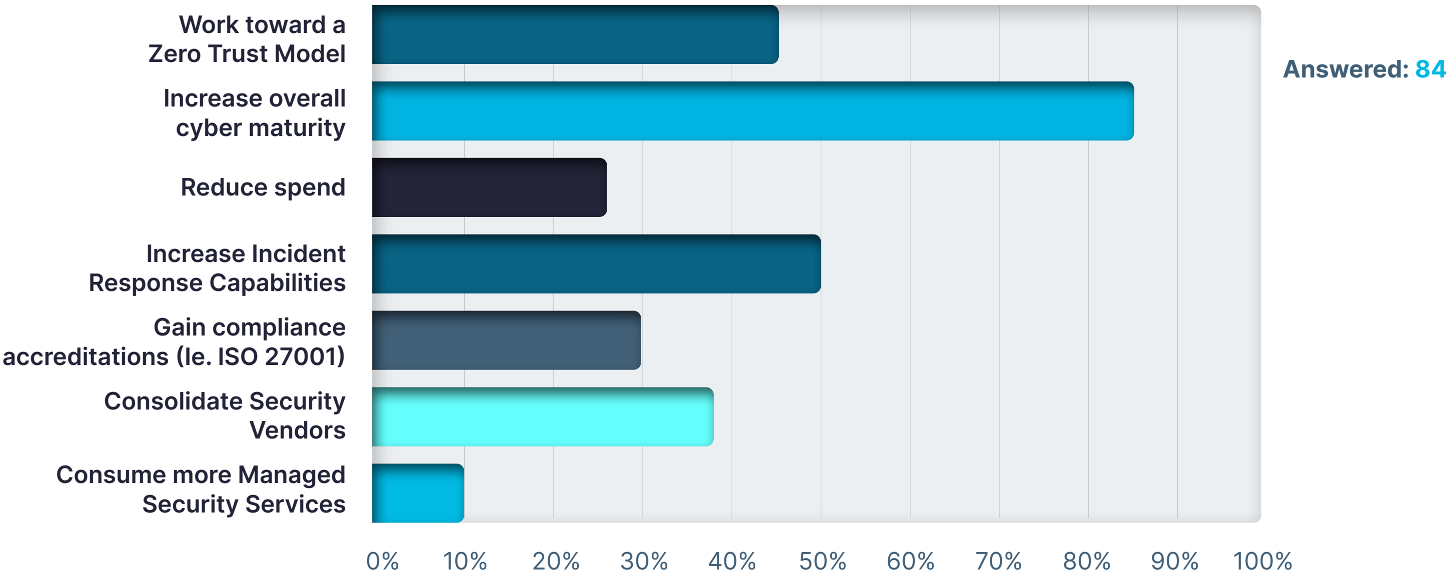
Organisations that are concerned about their ability to counter threats are advised to contact Bytes. Bytes can provide advice, guidance, and recommendations in this area. This will ensure that the relevant preparations are made.

A stand-out finding from this data is the concern around the Cyber Security Skills Gap. Bytes are seeing this as a big challenge as recruiting anyone is becoming increasingly expensive. When the recruitment fees, salary costs, security tools, training and shift work considerations are taken into account, it is often materially more cost effective to outsource all or part of the requirement to companies like Bytes.

Bytes have seen an increase in the relevance and requirement for outsourcing and managed services, primarily due to them being an immediate solution to the skills gap problem and can provide an immediate increase to security maturity.

Q2.

What are your top three cyber security priorities for 2023? Please select three options



Summary

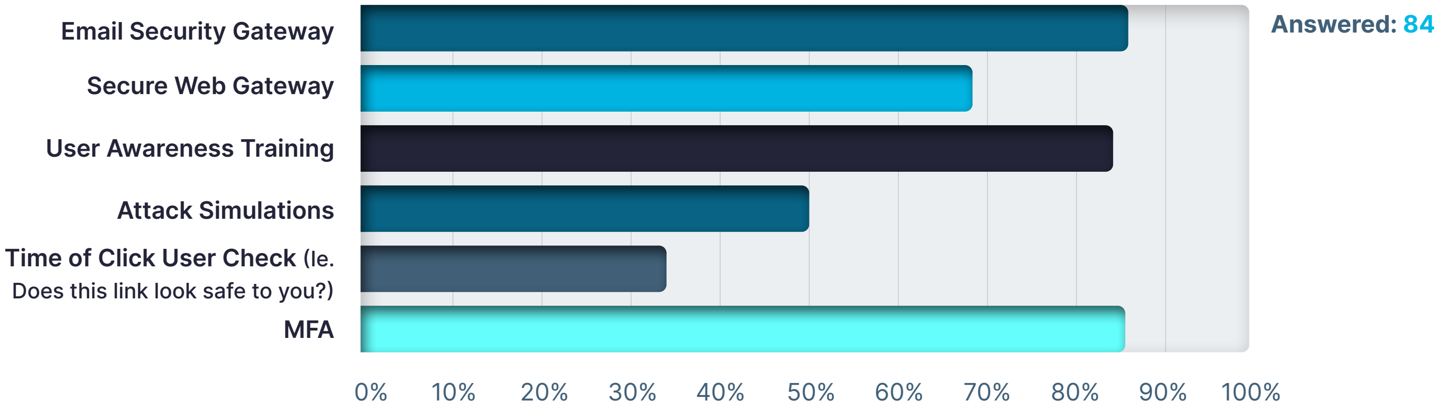
After many years spent encouraging organisations to prioritise the maturity of their security posture, it is very encouraging to see the messaging is now landing.

Through speaking with our customers, it has also been encouraging to learn that IT and Security are now rarely seen as a cost-centre, and, as a result, the pressure for IT and Security teams to find new ways to rationalise and reduce cost is starting to ease. Today, it is less about cutting spend and more about optimising investments. Security teams allocate more time to reviewing existing plans, establishing new ways of making smarter decisions. This review and optimsation is reflected in the strength of the answers around security solution consolidation.

The focus on incident response is also encouraging as organisations are now sharing the view of the broader security community that threats are an inevitability and are a question of when, not if. This mindset shift aligns with one of the Zero Trust principles that is to assume that you are breached. If organisations adopt this mindset they will make better investments to technology and factor in the people and process elements.

Q3.

What solutions/controls do you have in place to prevent/mitigate phishing attacks? Please select all that apply



Summary

The findings from this question can, mistakenly, be interpretated in a positive way. At first glance, the data highlights that 85% of organisations have Email Security Gateway, User Awareness Training and MFA in place to combat Phishing Attacks. It is pleasing to learn that a large number of organisations appreciate the value of each of these security components. However, it is important, and concerning, to note that up to 15% of organisations do not have any of these three critical areas in place today.

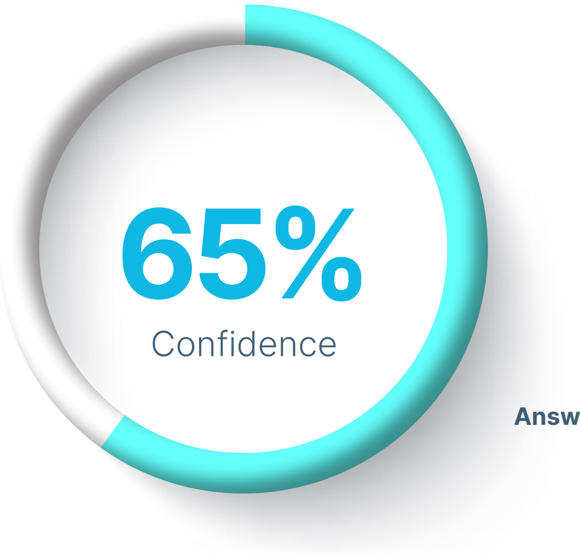
Every organisation should have MFA. It is no longer a nice-to-have but an essential component of any security environment. The same is true for Email Security Gateway – after all, every organisation uses email, and email is the biggest attack vector so every organisation should have a security gateway. These fundamentals are reflected in their inclusion in multiple compliance standards, and increasingly in Cyber Security Insurance requirements.

Q4.

What level of confidence do you have to prevent a phishing attack?

1% = Low Confidence, 100% = High Confidence

This means that on average people are 65% confident of preventing a phishing attack.



Answered: 83

Summary

Based on the findings from earlier questions, an average confidence level of 65% is not surprising. We would never expect 100% as we have never worked with any organisation that is that complacent, however, given 85% of organisations have MFA, an email security gateway, and a sufficient level of user awareness training, we would have expected the confidence level to be a little higher.

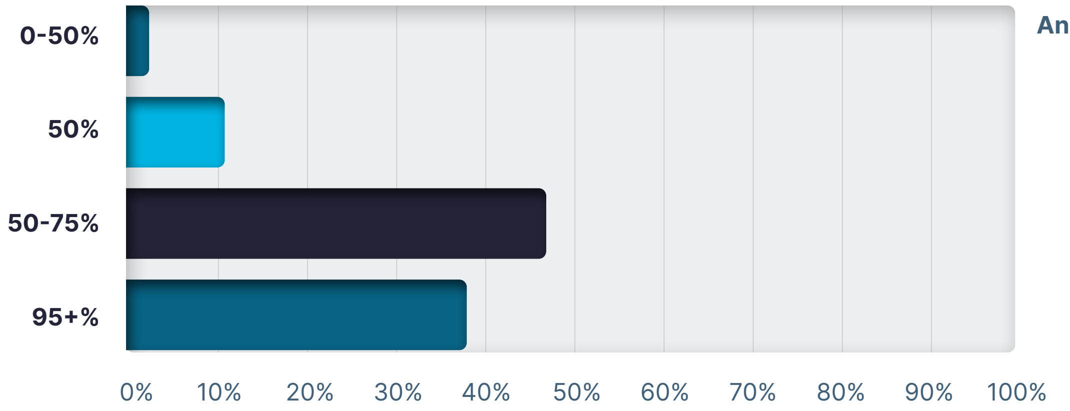
The reason for the low score is likely to be less about the security solutions organisations have in place, and more about a lack of confidence in the efficacy of them.

To help build confidence, organisations should be investing in assurance and testing services as well as simulated attack services as these will very quickly surface any vulnerabilities which can be addressed. The technology capability areas of “continuous testing” and “Attack Surface Management” have seen considerable development in the second half of 2022 and it is interesting to consider if this has been a response to, or driven concern in these areas.

Q5.

What percentage of threats do you think your email security solution is catching?

Please select one option



Answered: 84

Summary

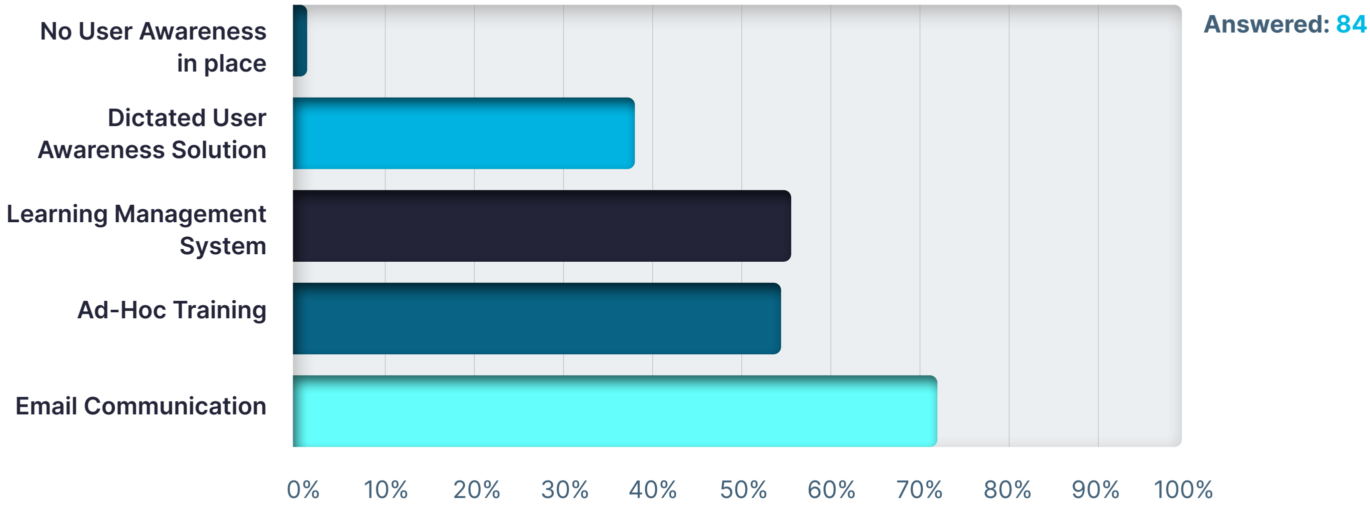
While on the surface it may seem encouraging that 47% of responders have confidence that >95% of threats are being captured by their email security solution, this does mean that 53% do not have this level of confidence. When choosing an email security solution, it is fair to expect it to capture around 98% of threats, so it does raise the question why organisations are lacking the performance they deserve.

Given that 91% of phishing attacks reportedly start with an email, if organisations are lacking confidence in their email security solution, they should adopt a layered approach to security. Layering complementary technologies throughout an attack kill-chain (such as the MITRE ATT&CK framework) is best practice as it is proven to materially reduce the chances of a breach.

Q6.

How does your organisation currently implement User Awareness?

Please select all that apply



Summary

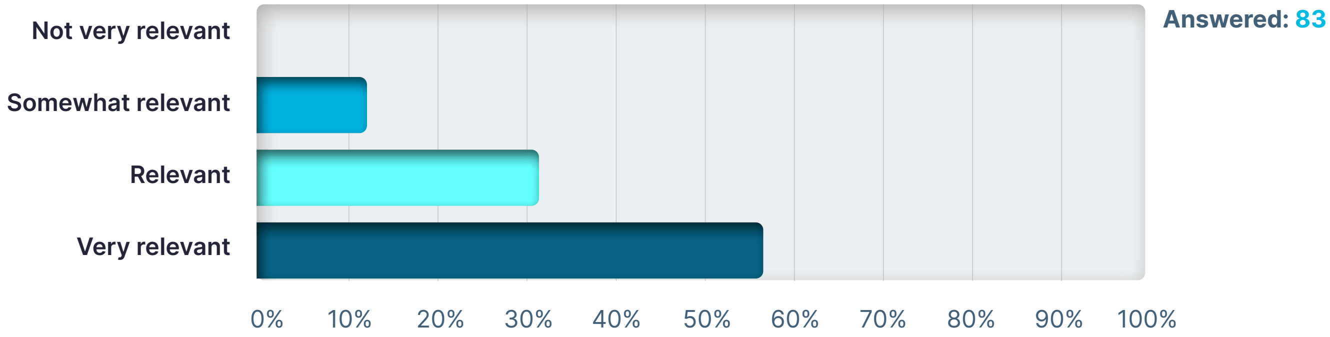
The first observation from the findings of this question relate to the number of responders that selected Email Communication. Email has an important role to play in the overall security posture of an organisation but should be used sparingly. Email should certainly be used to deliver phishing simulations and communicate general security awareness and competency-levels, however, there are better systems to use to deliver dedicated security training.

What is also alarming about the findings from this question is that more responders implement ad-hoc training than dedicated training. Best practice would suggest these should be flipped. Users remain the last line of defence against attack, so it remains essential that every employee understands the lengths attackers go to, and how to ensure they are part of the problem. The most effective way to achieve this is to ensure user awareness training is continuous, interactive, and engaging.

What is encouraging however, is that virtually every organisation is doing something around user awareness training. Providing this is not being undertaken simply as a tick-box exercise to appease the insurers or the auditors, but as a concerted and considered effort to mitigate risk, this is good news.

Q7.

How relevant do you think User Awareness Training is to being the last line of defense against a phishing attack? Please select one option

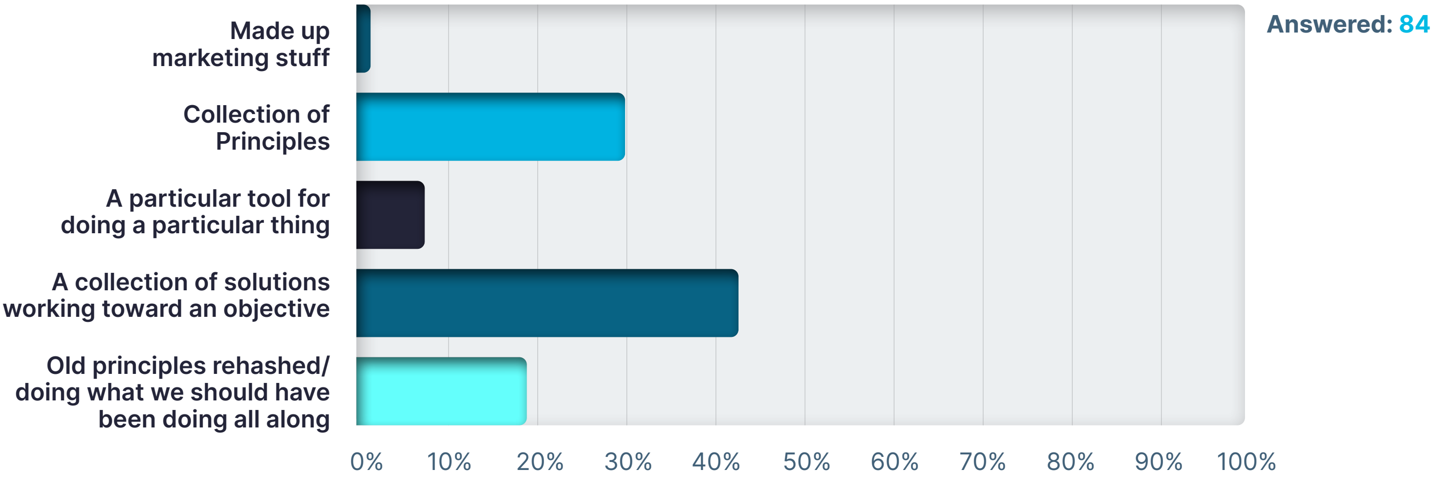


Summary

As stated previously in this Market Report, it is encouraging to note that a high percentage of respondents consider User Awareness Training to be either Relevant or Very Relevant. To maximise its value and effectiveness, organisations must establish and maintain a dedicated user awareness training programme.

Q8.

What is your opinion of Zero Trust? What do you think Zero Trust is? Please select one option



Summary

When we are asked this question, we respond by saying that Zero Trust is a Collection of Principles, however, it is good to see "A Collection of Solutions" at the top, most notably because it shows responders accept and agree that Zero Trust is not made-up Marketing jargon.

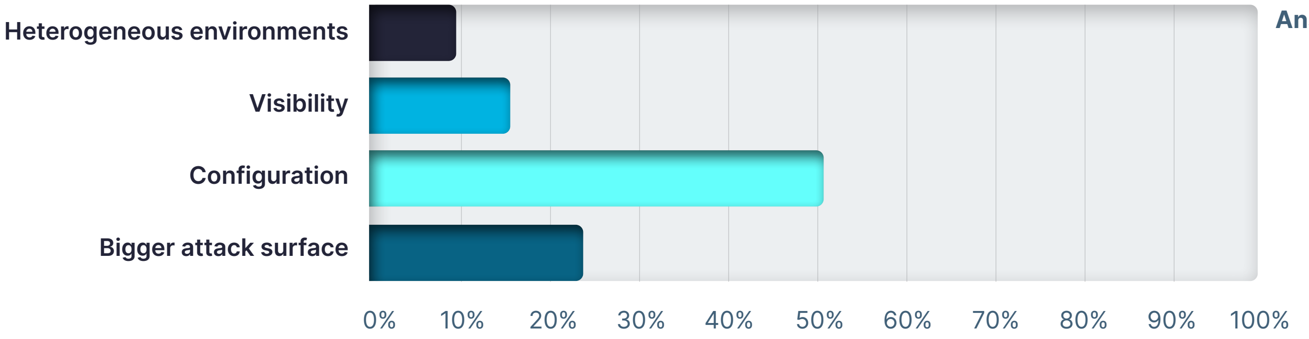
Our findings has confirmed that the confusion around zero trust is reducing, demonstrating an understanding amongst organisations that Zero Trust is a relevant approach, made up of the collection of principles that incorporates a collection of solutions.

It can also be argued that while "A Collection of Principles" is the "theoretically correct" answer, organisations need solutions to deliver against the principles and this is a useful practical definition.

Q9.

What do you perceive as being the biggest security risk to adopting cloud?

Please select one option



Answered: 83

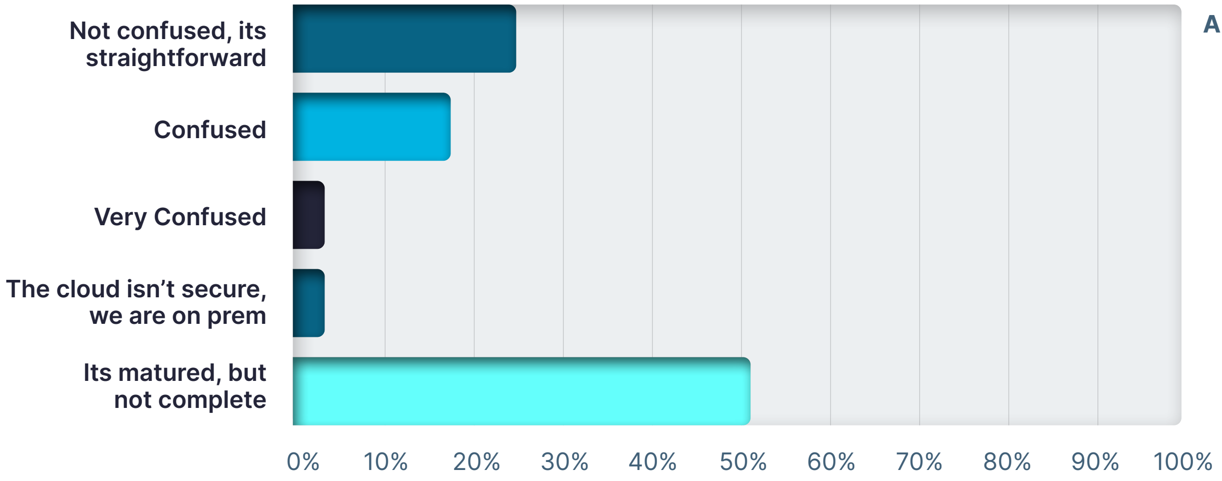
Summary

Unsurprisingly, Configuration is deemed the main risk to adopting cloud. The industry has been citing poor configuration as the main reason that security environments fail. It is a little surprising, however, that CSPM tools have not been more widely adopted as they have a material role to play in solving the Configuration challenge for cloud services. This could be that organisations are less worried about heterogeneous environments and are relying more on native tools. More investigation is needed to understand this.

We are slightly surprised that visibility is as low as it is, however, if this question was asked 3-4 years ago visibility would have been higher. This trend is evidence that both native and third-party tools have vastly improved.

Q10.

How confused are you with cloud security? Please select one option



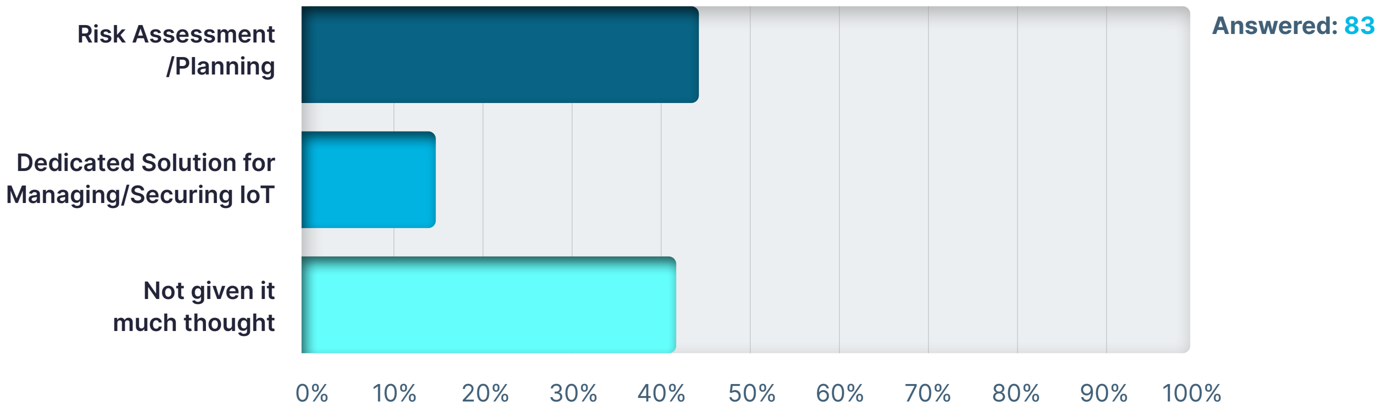
Answered: 83

Summary

Overall, our findings bear no surprise. Organisations are now mostly comfortable with the Cloud, and, to a greater and lesser extent, have the people, processes and technologies in place to ensure their cloud environments are secure.

Q11.

Given the changes in compliance and demand from business users/customers for IoT, have you put anything in place to mitigate the risk?



Summary

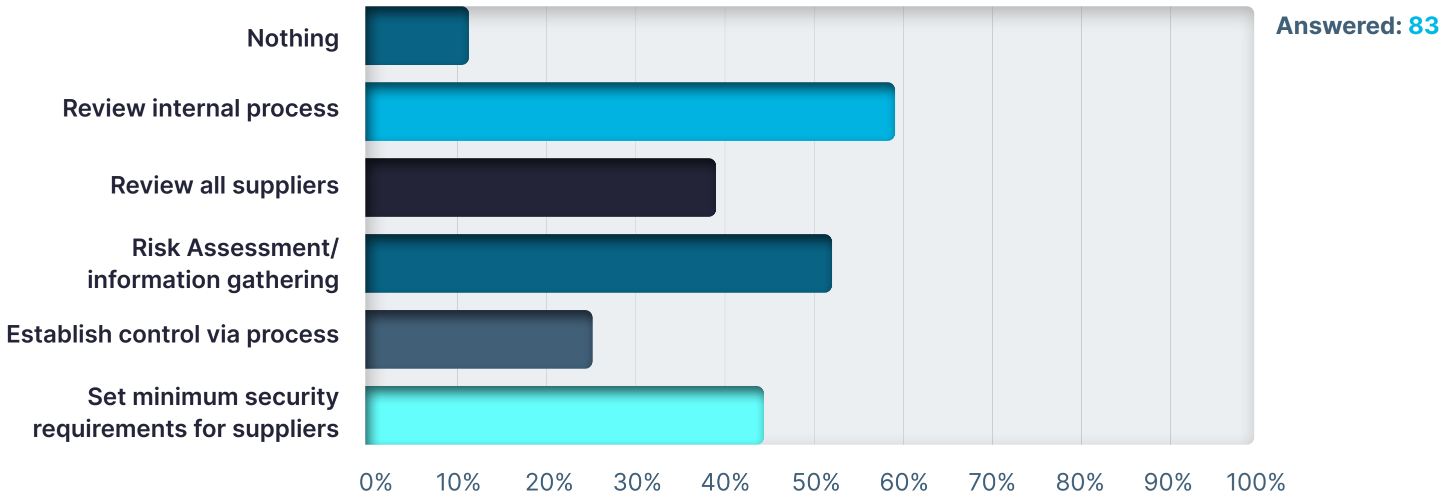
On the positive, it is great to see that 43% of organisations have undertaken Risk Assessments in relation to their IoT environment. It is also encouraging that 15% have a dedicated IoT security solution in place, though we would like to see this number a lot higher.

What is slightly concerning is that 42% of responders have not given IoT much thought. This contradicts the findings of the second question in which 85% of responders said they have "Increased Cyber Maturity" was one of their Security Priorities. Investing in a solution is not essential. However, if choosing to do so, making right, most informed decision is crucial, and a Cyber Risk Assessment must be undertaken. Bytes are able to provide dedicated support and guidance on this. Please reach out your Account Manager for more information.

Q12.

What actions have you taken in the past year to mature your supply chain security?

Please select all that apply

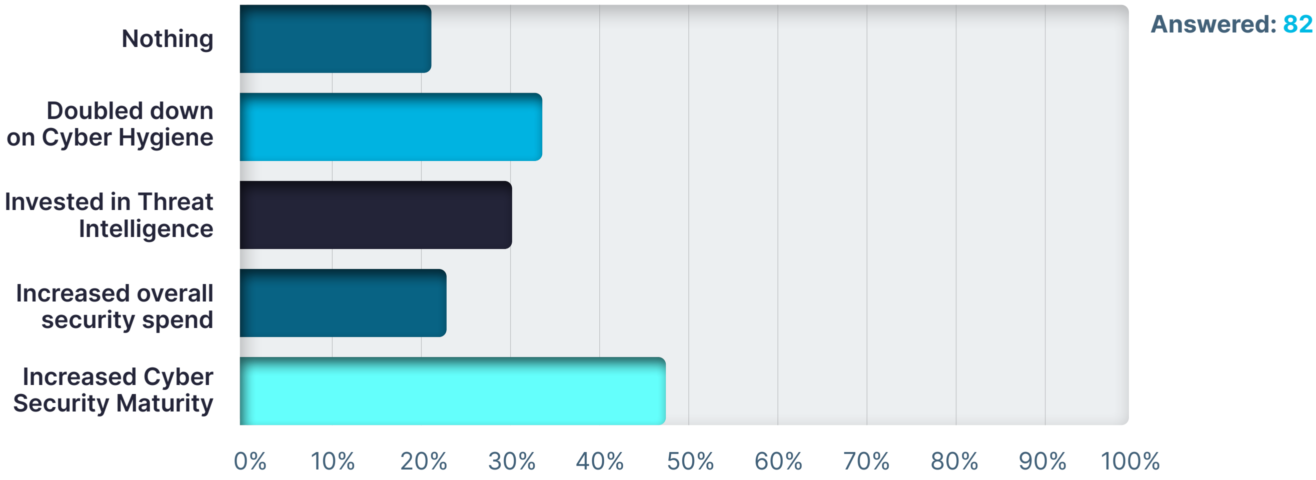


Summary

It is positive to see that in the past year activities are being completed to mature supply chain security. Due to the rapid rise in Supply Chain attacks, we encourage all organisations, little and large, to regularly review all their suppliers & service provider's security & risk management.

Q13.

Given the current war in Europe, changes have you made or plan to make to mitigate risk? Please select all that apply



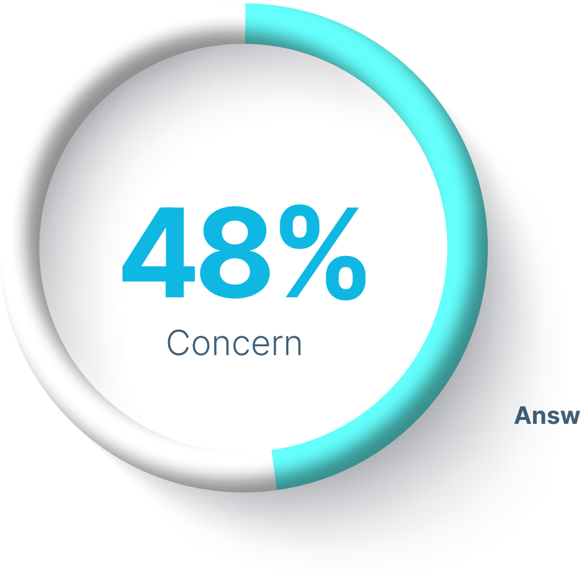
Summary

The responses of this question will require further investigation as it may be that all of those that responded "Nothing" already have a robust security posture in place, in which case changes may not be needed.

Our findings highlight that threats will become more prevalent, intelligent & tactical throughout 2023. Attacks can happen at anytime. It is incredibly important that all organisations are prepared for any scenario.

Q14.

How concerned are you about the security risks introduced by employees working from home? 1 %= Very Low Concern, 100% = Very High Concern



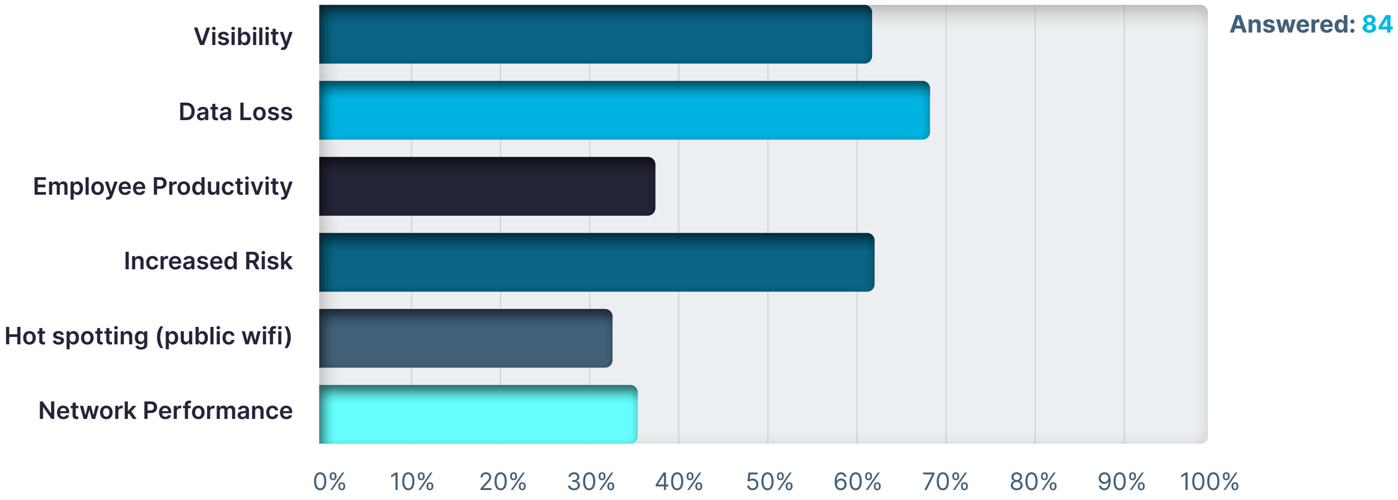
Answered: 84

Summary

When reviewing these findings against those from last year, the statistics are very different. Organisations appear to be less fearful of remote working and its impact on security. This is due to the stronger, more agile measures that have been put in place to improve and optimise security for remote workers.

Q15.

What would you consider are your organisation's top three main security challenges regarding supporting the remote workforce? Please select three options



Summary

While not new, it is no surprise that data loss remains a key challenge for many organisations. Our "CIS Gap analysis sessions" corroborates this and is evidence that effective DLP solutions are still not commonplace.

The interesting finding here is "Increased Risk" as 60% of responders say this is a key challenge and yet the findings of the last question contradict this. More research would be required to understand where this additional risk is originating from.

Conclusion

We would like to thank everyone who responded to our survey, the findings of which were very interesting and show that there is a concerted effort within organisations to improve their overall security posture and cyber maturity.

To ensure organisations put in place all the essential measures needed to prepare them for whatever threats they face through 2023, we highly recommend they undertake a Risk Assessment. Bytes can help in this regard.

If you would like discuss the findings of this Bytes Market Report with a specialist, or are keen to understand how Bytes can optimise your 2023 Cyber Strategy, reach out to your dedicated Account Manager, or email tellmemore@bytes.co.uk

About Bytes

Bytes provides leading insights, expertise and practical help to over 3,600 organisations nationwide. We enable effective and cost-efficient technology sourcing, adoption, security and management of software, hardware and cloud services.

Our UK business began in 1982 and has grown profitably each year to reach a turnover in excess of £1bn, making us one of the largest software services and solutions businesses in the country.

The most important aspect of our business is our people. We value initiative, teamwork and achievement. Together, we focus on providing the highest levels of service so we can deliver our ultimate goal – customer satisfaction and success.

Our customers include leading brands, such as Marks & Spencer, BBC, NHS, Clifford Chance, BUPA, Thames Water, Hiscox, Allen & Overy LLP and thousands more across retail, media, finance, manufacturing, legal, healthcare and the public sector.

We work closely with the majority of IT vendors and are delighted to regularly receive honours from them in addition to being named a Sunday Times Best Company to Work For 2020.

About Bytes Cyber Security

By acting as an independent, trusted advisor, our customers benefit from a wealth of knowledge that aids the delivery of an end-to-end and integrated methodology to cyber security. Our consultancy led approach enables our team to fully understand our customers challenges and business goals, ensuring we deliver innovative and relevant security solutions.

Bytes uniquely brings together cyber consultancy, solution specialists, pro-services and managed services under one roof.

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

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

BYTES | Smarter together