BYTES | Smarter together

The State of Cyber Security & Risk 2023

A Bytes Market Report
September 2023
In proud collaboration with Netskope

Introduction

By **Luke Kiernan** – Head of Cyber Security (Bytes)

Thanks to everyone who took the time to help shape our H2 2023 Cyber Security Report. By gathering insights into the current challenges, best practices, and solution adoption, this report aims to shed light on the evolving landscape of cyber threats and the collective efforts taken to mitigate them.

Here are some of the highlights for the report:

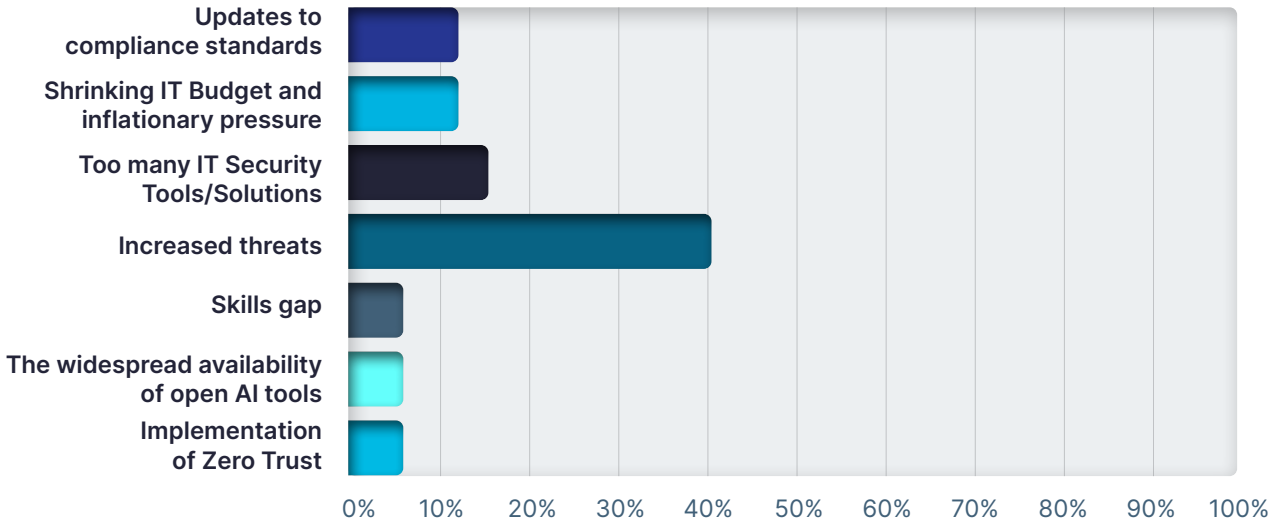
- **Zero Trust** is still high on customers priority list.
- The importance of User Awareness (training) & preparation when considering the use of **AI.**
- The **Cyber Skills Gap** continues to be a challenge. 40% of customers who responded have an Incident response plan, but no capability to respond.
- **Malware & Ransomware attacks** are considered the most significant risk.

This report includes expert views and commentary from Gennaro Migliaccio (Head of Solution Development at Bytes), Adam McCaig (Cyber Security Evangelist at Bytes) and Ian Paine (Solutions Engineering Manager, UKI at Netskope).

If you would like to 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

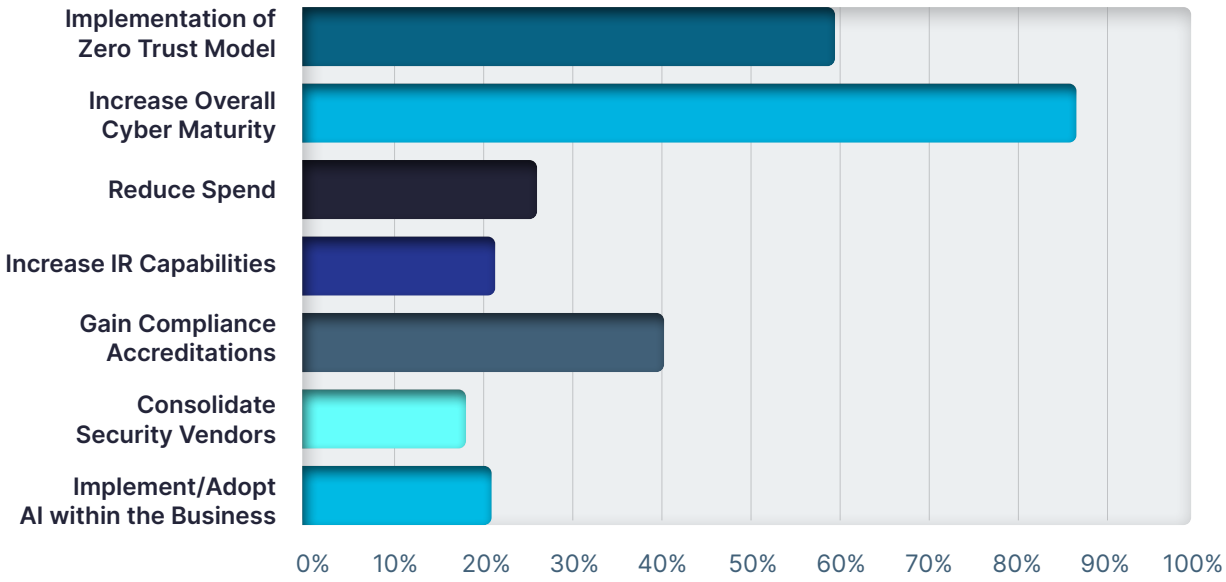
Given the constant drip feed of breach-related stories in the news, underpinned by the widely accepted hybrid working practices and use of cloud services, it is no surprise that increased threats are the most cited challenge here as IT teams are increasingly concerned by the potential for blind spots in their security posture.

What is a little surprising is that “Skills gap” is so low, as that is often mentioned when speaking to customers. The skills-gap challenge is partly due to the ongoing recruitment issue within the cyber security market and partly due to the evermore complex environments that organisations need to support.

“Too many IT Security tools and solutions” is very much part of the skills-gap conversation and comes in second. Our customers are often citing the direct correlation between “Too many IT security tools” and the “Skills gap”, as often too much avoidable pressure is placed on IT teams due to the number of different solutions that need to be learnt and operated. Having fewer vendors often means there is commonality between user-interfaces which in turn can materially ease the skills-gap issue.

Q2.

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



Summary

Increased overall cyber maturity is way up the list here as it is very much a blanket answer. If that is not on your agenda, then you are doing something wrong.

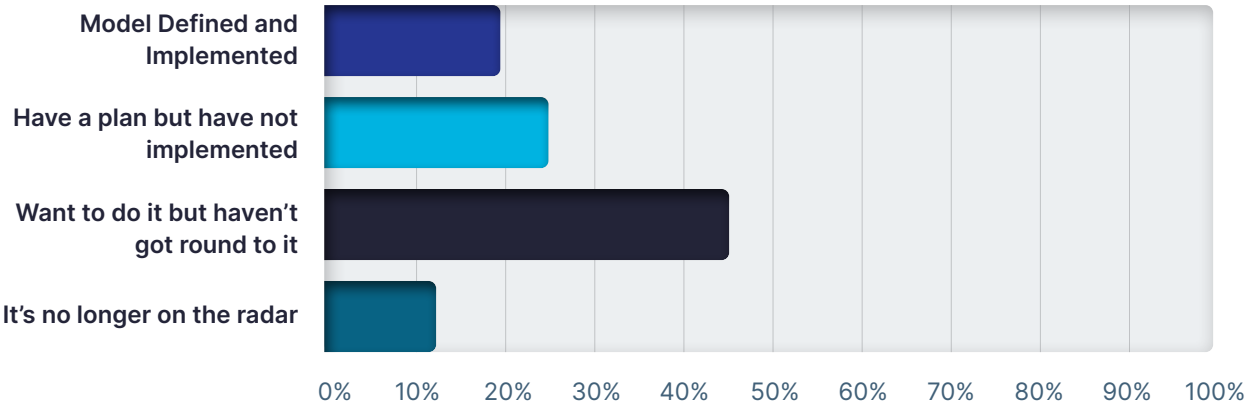
What is a surprise here is how many respondents did not rate "Consolidate Security Vendors" higher. As mentioned in the previous question, vendor consolidation has many benefits, with common user-interfaces and reduced blind-spots being two, thereby easing the training and risk exposure challenges retrospectively. Complexity is also expensive, especially if some of the vendors have on-premises solutions that need constant hardware and software maintenance, and some have cloud solutions, that bring their own set of challenges.

It is reassuring to see "Implementation of Zero trust model" coming in second. With AI being spoken about a lot, we tend to hear less about Zero trust, so it is encouraging to see it is still a business priority and that businesses are still actively working towards this model.

On the topic of AI, it is surprising it is only registering about 20% here as there is a lot of hype and buzz regarding AI from lots of providers, and vendors. This could be because we are only scratching the surface with AI. There are many open AI tools that anyone can use but nothing that is off the shelf and "business grade" today, that being, AI tools that have the capability of providing results from your dataset, without the requirement of configuring an AI solution from the ground up. Most of our customers are telling us they are waiting for the copilot stack from Microsoft to come out. That is the milestone when people will start taking AI seriously.

Q3.

What is your current progress on Zero Trust? Please select one option.



Summary

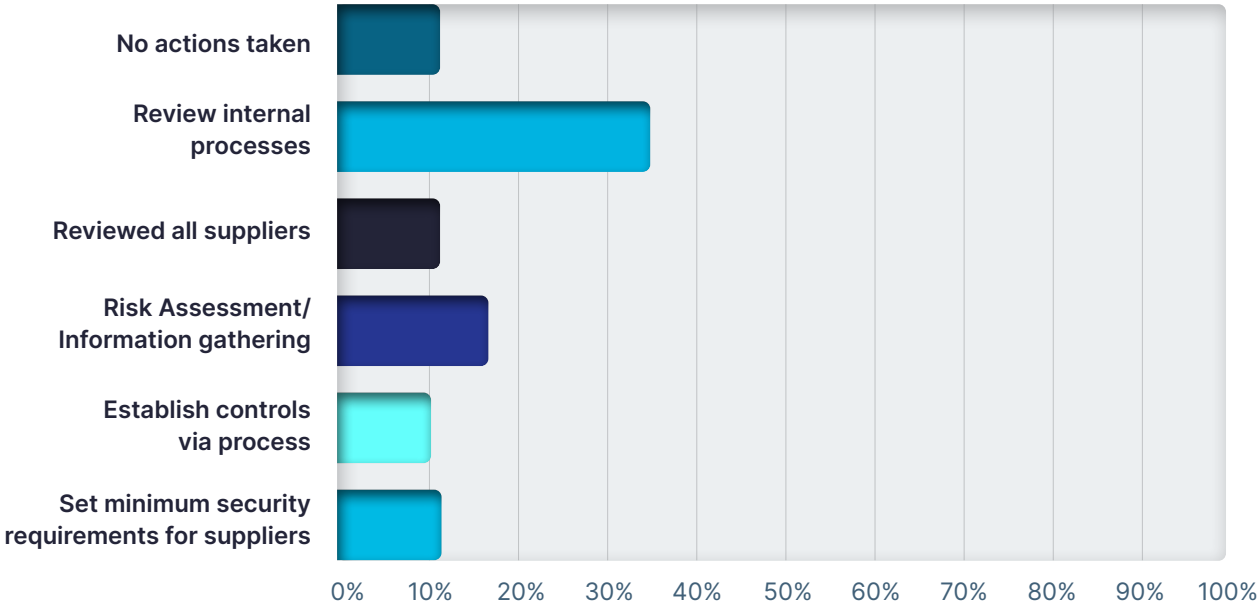
If we remove the 12% of respondents who selected, "It's no longer on the radar" it leaves 88% of organisations stating they are doing something – this is encouraging, though when you dig a bit deeper almost 45% of respondents "Want to do it but haven't got round to it". It is a little worrying that so few have a plan. This falls somewhat in line with the last question, that Zero Trust is a priority for 2023, however we would have expected to see a larger portion of responses that have some form of plan given that we are more than half way through the year.

Zero trust has been talked about for around 9-12 months now so if we were to rerun this survey in 6 months, we would expect more people to have a dynamic plan consisting of a structured set of objectives they intend to proceed with in the next year that moves them towards zero trust.

Q4.

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

Please select one option



Summary

In most cases, business partners should be part of your risk profile. This view is shared by the BSI and NCSC. It is therefore encouraging that 87% of people are doing something to mature their supply chain security.

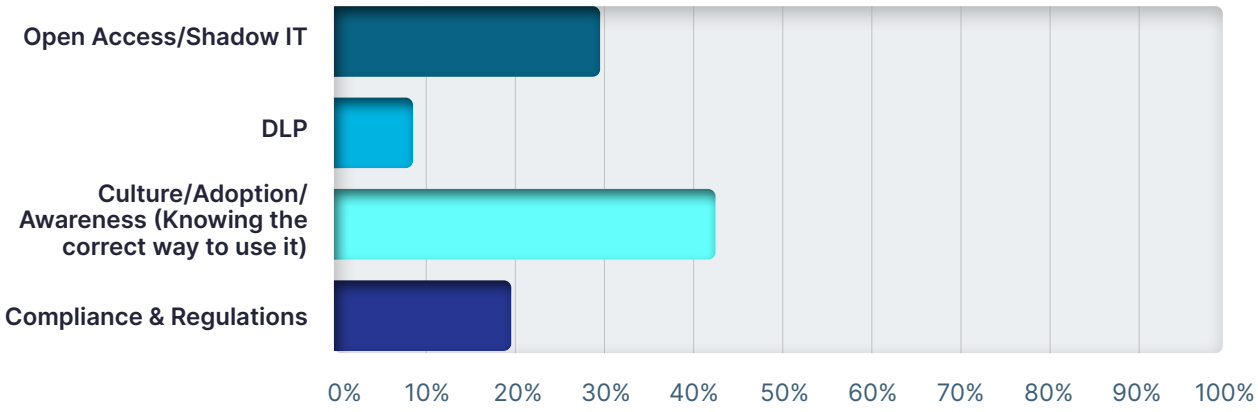
While encouraging, this is not that surprising as there have been a lot of breaches reported recently where a third-party was responsible, the recent Metropolitan Police incident is a good case in point as it was not the Met that suffered a breach, but the contractor they use to produce their warrant cards that was breached.

It is also interesting that supply chain security is featuring more on tender documents and frameworks and is often scrutinised as part of a supplier selection process.

Q5.

What do you foresee as the biggest security challenges with AI?

Please select one option



Summary

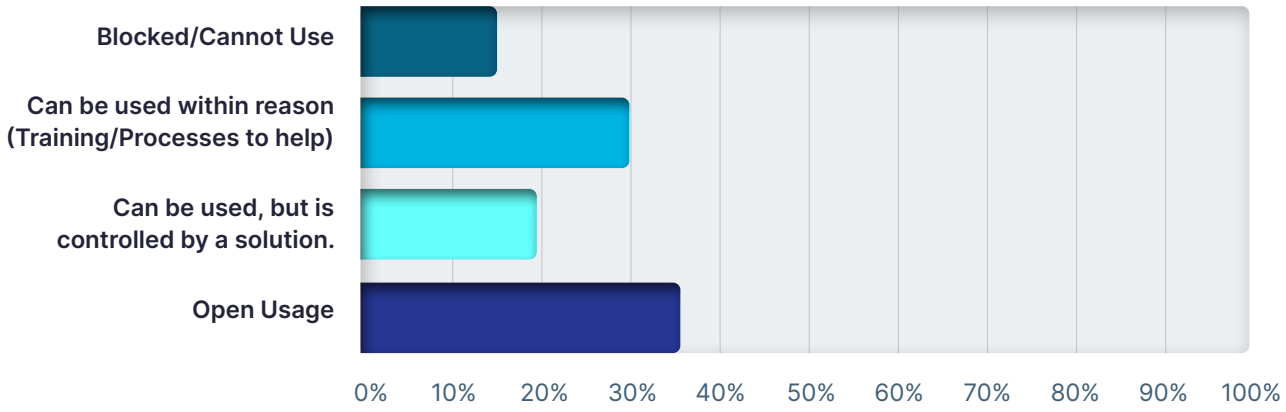
The findings from this question are contrary to what our customers are telling us, particularly in relation to DLP. Most of our customers are not necessarily against using AI, they just do not want their sensitive data and intellectual property being used by an open AI tool as it increases the DLP risk. This view aligns with the previous question about supply chain scrutiny and suggests DLP should be higher up the list.

What is interesting from the findings of this question is the importance of awareness. Training employees on the pros and cons of AI is essential as it will be through education that the benefits will be realised, and the risks mitigated.

Q6.

What is your current stance on the business utilising AI?

Please select one option



Summary

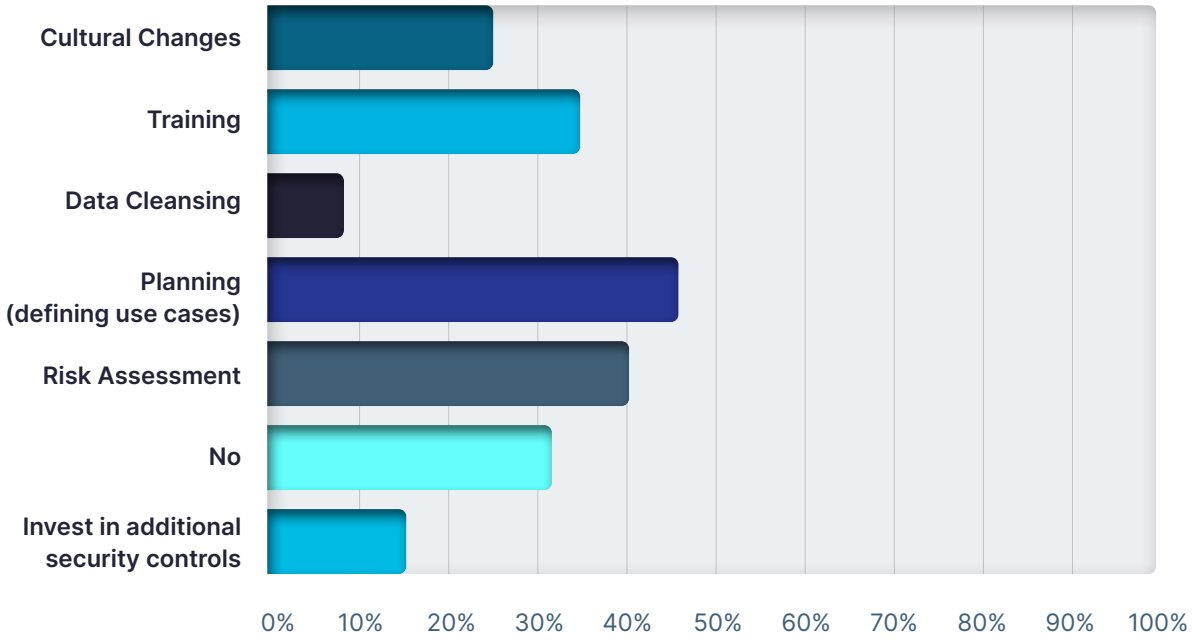
It is evident that most IT professionals are supportive of AI being used within their IT environments, but within a controlled or limited capacity. This finding aligns well to the last question and supports the notion that there are concerns with AI if it is left unchecked – particularly with regards to the potential loss of company data.

Organisations recognise the benefits of AI but want to make sure the necessary policies and processes are in place and that employees are properly trained before people are let loose on it. The reality is, it is very hard to stop anyone from using AI tools because even if websites are blocked, people will find workarounds as they do with other shadow IT systems.

Q7.

Have you completed or are planning to complete any preparation steps for AI?

Please select all that apply



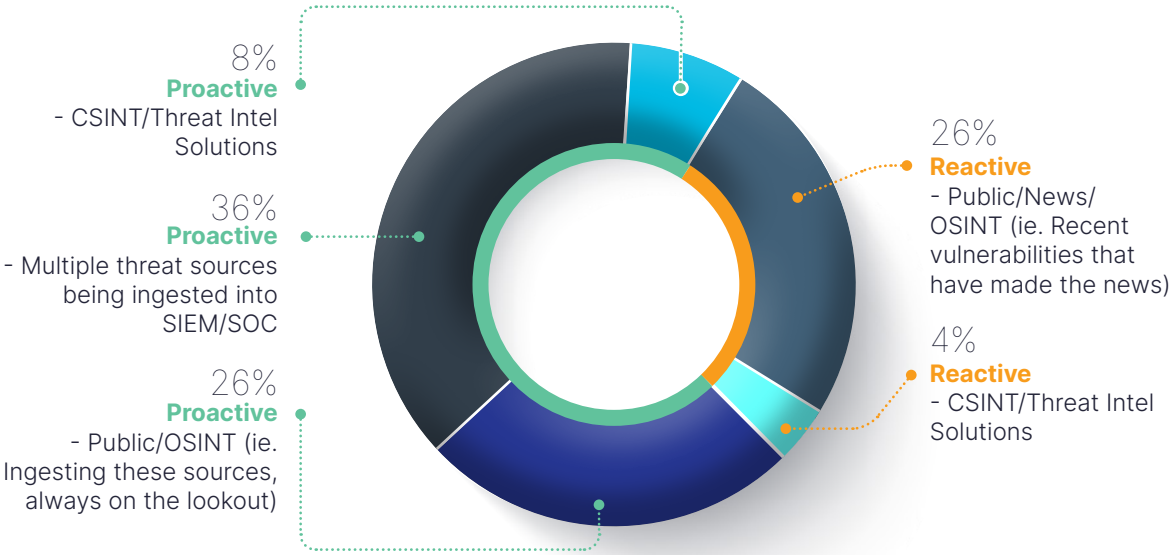
Summary

Taking time to plan, define use-cases and perform risk assessments is certainly best practice here, followed closely by Training. This process-flow is certainly the norm and aligns with most IT change and adoption programmes. It also removes or reduces the need for organisations to block specific websites as people will be more aware of the pitfalls and risks that it poses to their business.

What is of slight concern in the findings from this question is that a third of all respondents have not completed any preparation steps for AI. Given the open access to AI solutions, many of which have free-to-use versions, and the amount of publicity, it makes sense for organisations to put in place risk-prevention awareness programmes. There is an equally compelling argument that the more employees understand about some of the legitimate AI tools on the market, the more productive and competitive they will be.

Q8.

What threat feeds are you currently utilising and how?



Summary

It is reassuring to see that most respondents are proactively ingesting multiple threat sources into a SIEM/SOC. This is something we have been advising our customers to do for a very long time, so it is good to see that many organisations are now taking this stance.

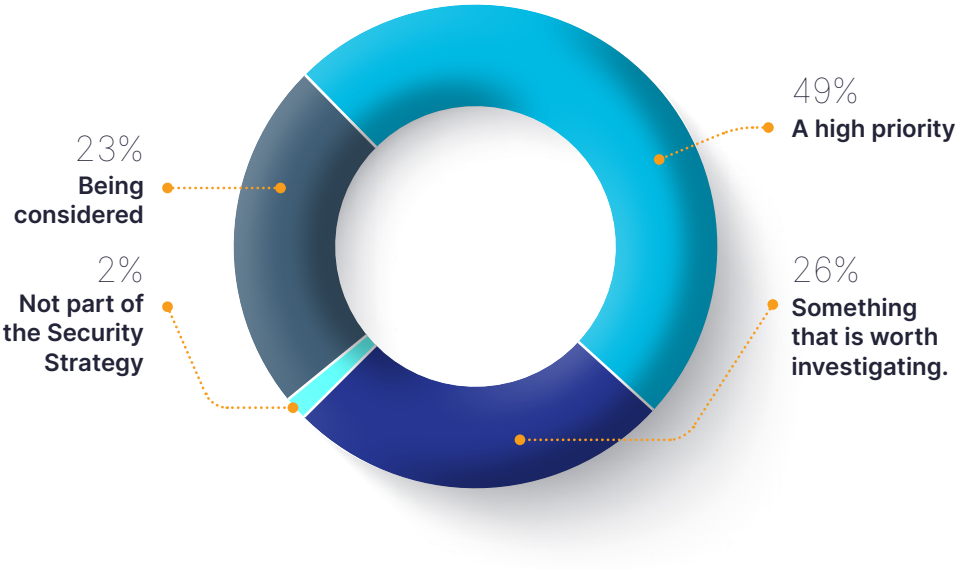
The reason it is important is that you can read the news or security portals and understand what vulnerabilities are being exploited. You can also go a step further and look at digital shadows and other closed-source intelligence sources to learn that a particular threat-group is doing something or that there is a new variant of malware/ransomware doing the rounds, but then doing something with that intelligence is the next step.

Ingesting that information into a SIEM/SOC solution to enrich the data is the key and is what makes the material difference to enhancing an organisation's security posture, so it is very good news to see a growing number of organisations doing this.

Q9.

For 2023, Is threat intelligence:

Please select one option



Summary

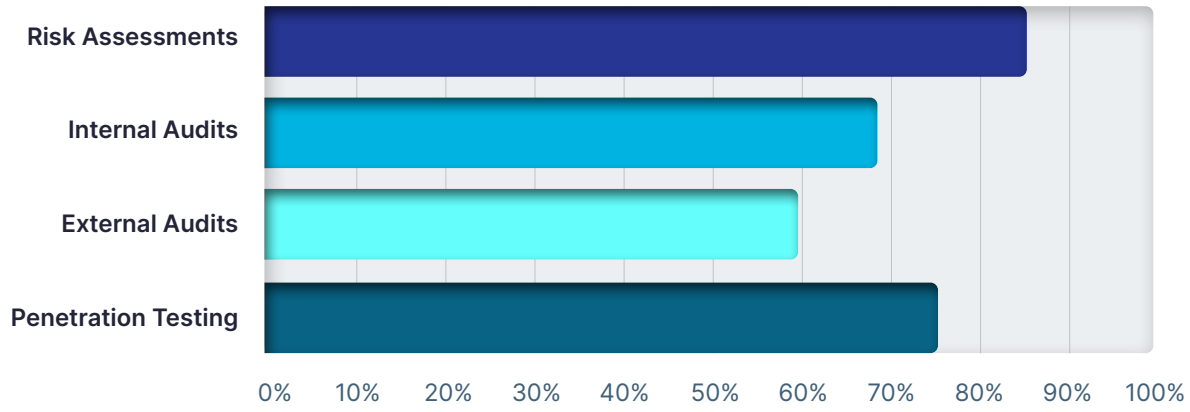
It is no surprise here that almost 98% of respondents consider threat intelligence as important in some capacity, although this should be 100% as anything other than that means that some organisations are opening themselves up to avoidable risk.

We cannot fight what we cannot see or know. Using Threat Intelligence is a key method to providing insight to the potential risks and vulnerabilities that an organisation could face.

At Bytes we have customers talking about this daily and asking how threat intelligence can be plugged into their SIEM/SOC, or in some cases, making it part of a managed service.

Q10.

How do you measure your risk management? Please select all that apply



Summary

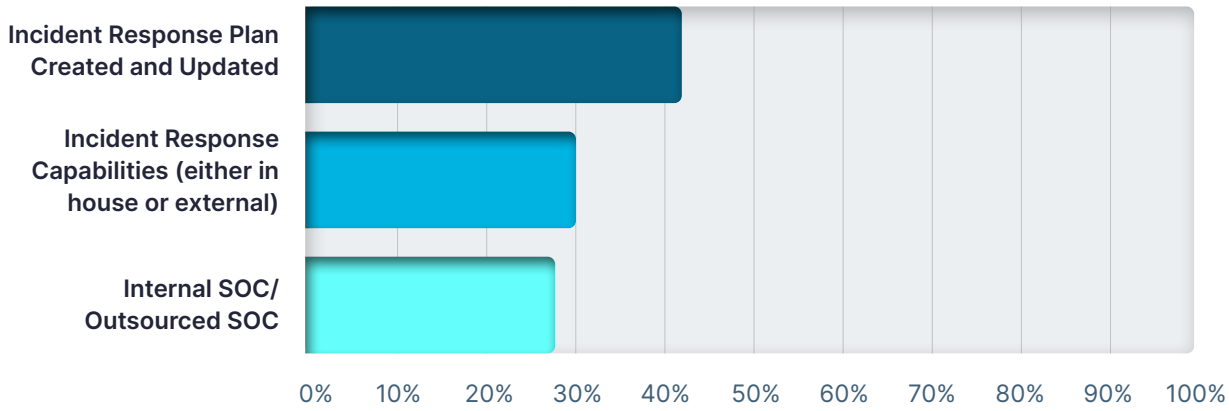
It is a little alarming that as many as 25% of respondents are not doing any Penetration testing. Every organisation should be penetration testing. The same is true with risk assessments. Every organisation should be doing them, and yet according to these findings, 15% of respondents are not doing any risk assessments. Discovering and establishing your risks and vulnerabilities is crucial to continuously improving your security maturity.

Pen tests are expensive so the cost can put people off, however, risk assessments can mostly be conducted internally. Understanding what the risks are and how to address them is literally the foundations of building a robust security strategy.

The number of organisations conducting audits, whether they be internal or external is very encouraging and is an increase on previous survey's we have conducted. This speaks to the fact that more and more organisations are aligning themselves to security frameworks and are actively auditing to ensure compliance.

Q11.

What level of preparation has been completed to effectively respond to Cyber Incidents? Please select one option



Summary

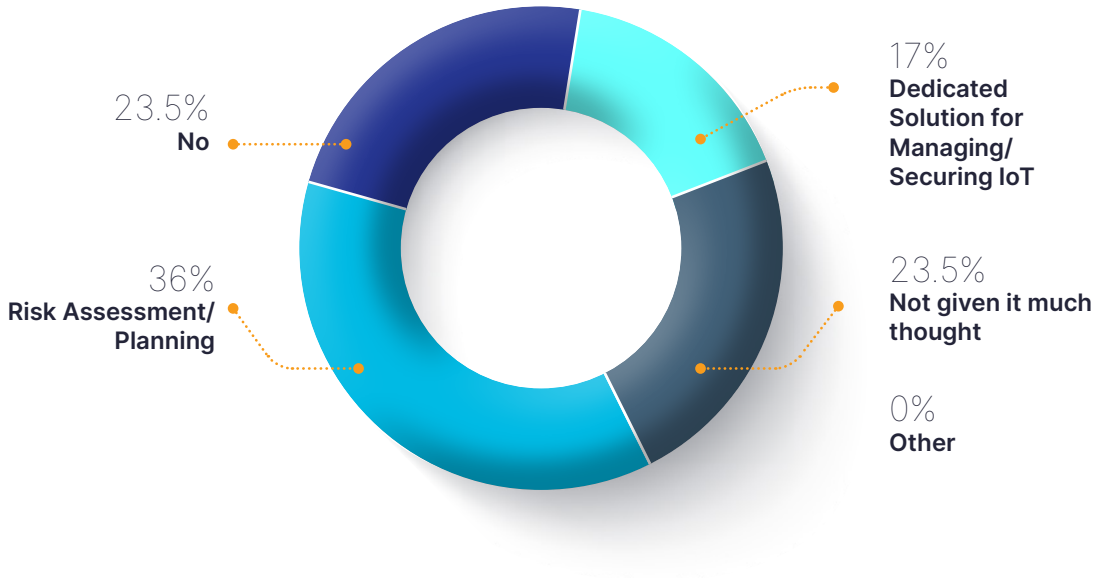
Having a plan is the foundation of any and every incident response strategy but having a plan doesn't necessarily mean you can respond to an incident effectively. That is why the next option around capabilities is important.

In isolation the 30% needs to be significantly higher as this figure suggests that if there is a serious incident only one in three organisations have the capability to deal with it. What is encouraging however is that almost a further third of organisations have an internal or external SOC that would be able to deal with that.

It still means that over 40% of organisations have a plan but no capability to respond. From an attacker's perspective those are very good odds and a potential gold mine for them.

Q12.

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



Summary

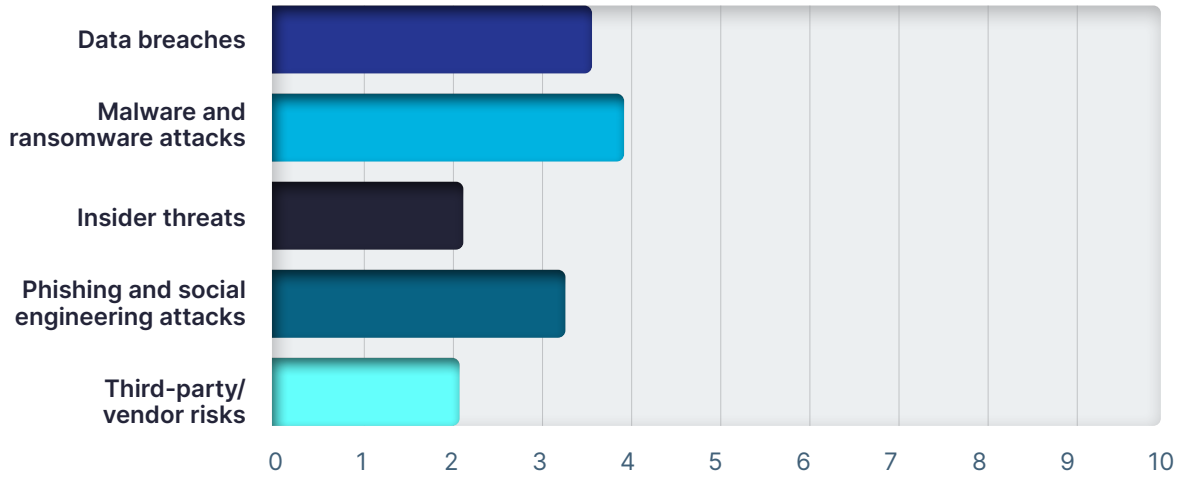
While 23% of organisations say they have not put anything in place to mitigate the risk associated with IOT, it is not that much of a surprise as IOT tends to be treated differently than your typical workstations and devices. This could also be answered by organisations that simply do not have IOT, as it tends to be vertical specific.

Whilst the percentage of dedicated solutions is lower than we would expect, we would also need to consider that more and more vendors are broadening their security portfolio with some including IOT capabilities. This could mean that businesses do not have a dedicated solution as they are leveraging existing products, on the flip side, this also means that organisations may have capabilities they are not aware of to protect IOT environments but have not rolled this out.

Whare IOT strategies are more prominent is in certain verticals, such as the Healthcare industry & Manufacturing, as there is a wider scope for specialist machines/devices. Those that are in these verticals should consider security controls around IOT.

Q13.

Which of the following cyber risks do you consider most significant for your organisation? (in order of severity)



Summary

Before we provide some analysis of the findings from this question it is important to consider the movement of data over the past decade. Ten years ago, data was predominately kept within the network perimeter, so it was significantly easier to manage. Today, data largely resides outside of the network perimeter so is more prone to attack.

It follows therefore that malware and ransomware attacks are considered the most significant risks, with data breaches being a close second. These align with the conversations we are having with our customers, partly due to the continuing high-level breaches that are we hear about in the news on a weekly basis.

Organisations are still very much concerned about phishing and social engineering attacks, and with the increase in AI being used to orchestrate attacks, this means of a gateway into an environment is only going to be more successful if left unchecked.

Q14.

How frequently does your organisation review and update its cyber risk management strategy? Please select one option

Summary

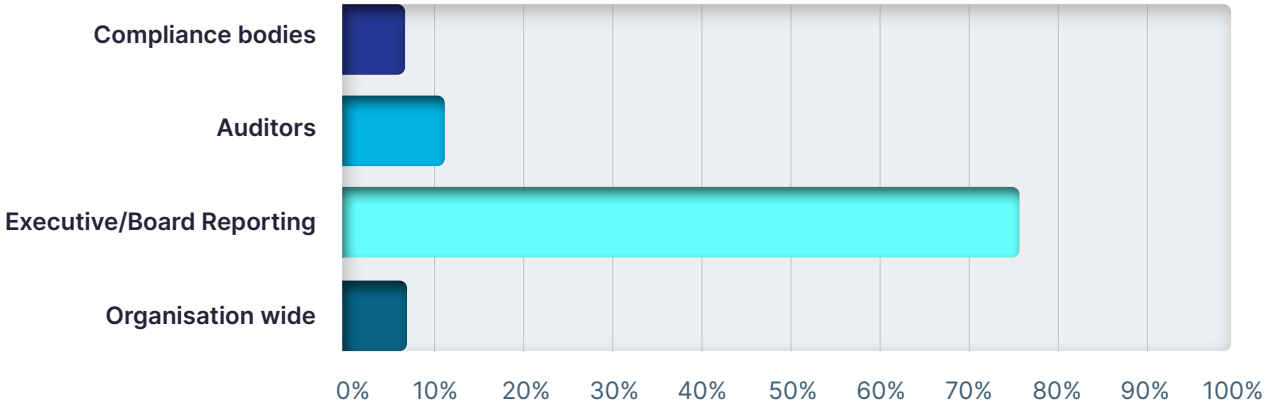
The findings of this question are interesting. What we see from our customers is that most update their documentation annually but review more frequently. This may be the case here but would need further investigation to conclude either way.

What we do not see are many customers conducing a full review quarterly as this can be very time and resource heavy, however if there is a serious incident then changes are often made following a lessons-learnt exercise to ensure a repeat does not happen. This of course is very different to the 2% of organisations here that state they only update their cyber risk management when a significant event happens. This is not a recommended way of working.

Whilst the question states to select one option, a good approach is to review your strategy periodically, but also include changes as you go in the form of lessons learnt. This way, your strategy is evolving in line with any threats or incidents that have arisen.

Q15.

How (and to who) does you organisation report risk? Please select one option



Summary

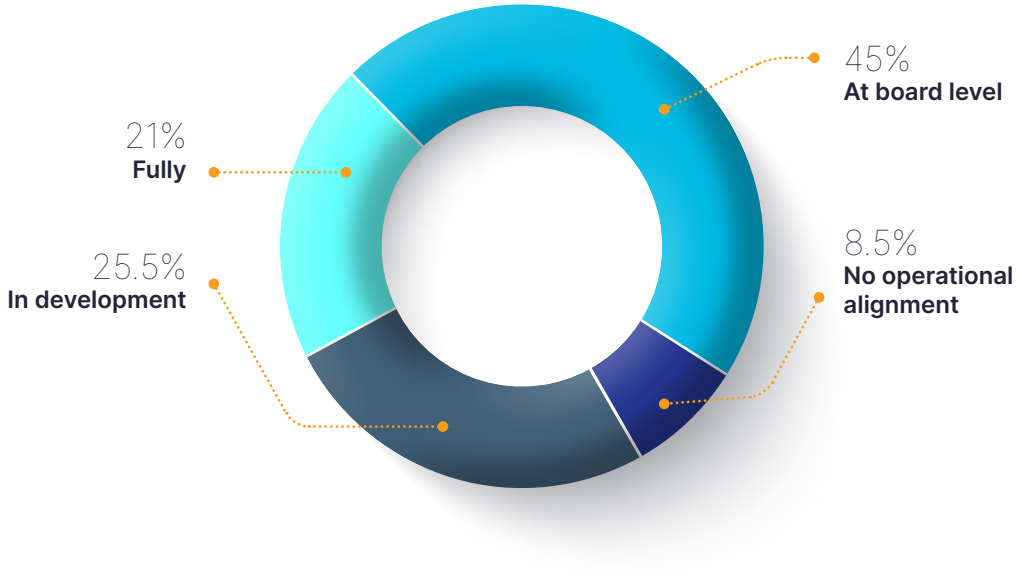
It is encouraging that Executive teams are taking (and many cases maintaining) an interest in risk, as ultimately accountability resides with the Board.

What we see is that if it is an IT or technical risk then the CTO is normally accountable, whereas if it is financial or accounting based, then normally the accountability resides with the CFO.

There are of course going to be crossovers, such as in the case of a ransomware attack, in which case you typically have the CTO, CFO, and CISO all involved, with any actions overseen by the CEO. If the breach is very serious, then the CMO is also part of the remediation strategy as customers and shareholders need to be updated in a timely and responsible manner.

Q16.

How integrated are your Cyber risk and Business Risk (including ESG etc) programmes?



Summary

There is a split of answers here. What is clear from these findings and our own customer discussions is that it is at Board level where cyber risk and business risk starts to combine. This is supported in these figures as only 8% of respondents have no operational alignment between Cyber risk and Business risk.

This 8% figure is quite remarkable as means 92% of organisations have some level of alignment. This was not the case 12-24 months ago when cyber risk and business risk were very much separate.

Bytes Cyber Insights

Our Cyber Insights pillar is shaped by three core areas - client feedback, industry research and expert advice. In combining research from across each area, Bytes deliver valuable insights, guidance and recommendations across the entire Security & Risk landscape. Helping to ensure our customers remain resilient against the latest & emerging threats of today's modern world.

To find out more about our latest Cyber Security & Risk customer events, conferences, and roundtables, please visit: **https://www.bytes.co.uk/**

To explore our Cyber Security workshop portfolio, please visit: **https://www.bytes.co.uk/security/cyber-consulting-services/cyber-security-portfolio**

Our expert contributor – **Netskope**

This report has been created in collaboration with a Bytes leading Cyber Security partner, Netskope.

Netskope are recognised as a Leader in the 2023 Gartner® Magic QuadrantTM for SSE.

Netskope help organisations stay ahead of cloud, data, and network security challenges.

Cloud transformation, hybrid work, cybersecurity risk, and operational efficiency have changed how security and connectivity need to work.

Netskope sees and understands these changes and works with organisations to protect and empower people and data anywhere they go, no matter what.

To learn more about our partnership with Netskope, and how we can help your organisation transform your Cyber Security, please reach out to your dedicated Bytes Account Manager, or email our friendly team via tellmemore@bytes.co.uk

Conclusion

Many thanks to those who contributed to the research and development of this report. Customer insight and feedback truly goes a long way in helping Bytes to understand and provide relevant guidance to support each customer journey and cyber transformation.

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